НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

факультет інформатики та обчислювальної техніки
(повна назва інституту/факультету)

кафедра автоматика та управління в технічних системах _____
(повна назва кафедри)

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ О. І. РОЛІК
(підпис) (ініціали, прізвище)
“ ___ ” _____
2018 р.

Магістерська дисертація

зі спеціальності (спеціалізації) 126 «Інформаційні системи та технології»
_____
(код і назва спеціальності)

на тему: Система аутентифікації на базі еліптичних кривих з використанням векторних операцій _____

Виконав : студент 6 курсу, групи ІА–73мп
(шифр групи)
Альбрехт Йосип Омелянович _____ _____
_____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент, к.т.н. Полторак В.П. ____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

АНОТАЦІЯ

В даній роботі 92 сторінки текстової інформації, 34 рисунки та 35 таблиць.

Актуальність даної роботи полягає у суттєвому зменшенні необхідної довжини ключа для реалізації електронного цифрового підпису за рахунок використання еліптичних кривих, визначених у трьох вимірах, при збереженні рівня криптостійкості, і збереженні швидкодії за рахунок використання векторних операцій

Ключові слова: система аутентифікації, еліптична крива визначена у трьох вимірах, векторні операції, цифровий підпис

The relevance of this work is in significant reducing the required key length for the implementation of the digital signature through the use of elliptical curves determined in three dimensions, while maintaining the level of cryptostability, and maintaining the performance through the use of vector operations.

Keywords: authentication system, elliptic curve determined in three dimensions, vector operations, digital signature

ЗМІСТ

СПИСОК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

API – Прикладни́й програ́мний інтерфе́йс (англ. Application Programming Interface, API) — набір визначень підпрограм, протоколів взаємодії та засобів для створення програмного забезпечення.

ECDSA – (Elliptic Curve Digital Signature Algorithm) - алгоритм з відкритим ключем для створення цифрового підпису, аналогічний за своєю будовою DSA, але визначений, на відміну від нього, не над кільцем цілих чисел, а в групі точок еліптичної кривої.

Аутентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

Двофакторна аутентифікація – розширена аутентифікація, метод контролю доступу до комп'ютера, в якому користувачеві для отримання доступу до інформації необхідно пред'явити більше одного «доказу механізму аутентифікації». До категорій таких доказів відносять

Еліптична крива – це множина точок проективної площини над K, що задовольняють рівнянню:

$$y^2 = X^3 + AX^2 + BX + C$$

ЕЦП – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Криптостійкість – рівень захищеності криптосистеми

ОС – це базовий комплекс програм, що виконує управління апаратною складовою комп'ютера або віртуальної машини; забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем.

Скінченне поле або поле Галуа — поле, яке складається зі скінченної множини елементів.

ВСТУП

Одним з чотирьох елементів криптографії є аутентифікація. Аутентифікація це спосіб довести приналежність певної інформації до конкретної людини. До ери комп'ютерів для аутентифікації використовували підпис, відбиток пальця, печатку, штамп тощо.

З появою асиметричного шифрування з'явилась можливість проводити цифровий підпис даних. Всі методи аутентифікації реалізовувались в скінченному полі Галуа з дійсних чисел.

З року в рік обчислювальна здатність комп'ютерів тільки зростає. Якщо в 2008 році найпотужніший комп'ютер Roadrunner на піковій потужності виконувала 2.3 Pflops операцій, то на сьогодні найпотужніший суперкомп'ютер на піковій потужності виконує 187.7 Pflops операцій. За десятиліття обчислювальна потужність найпотужнішого комп'ютеру виросла на два порядки. Це означає, що для забезпечення того ж рівня криптостійкості алгоритми шифрування та аутентифікації повинні використовувати ключі більшої довжини. А відповідно витрачати більше енергії і часу для проведення потрібних операцій.

На сьогоднішній день використовуються алгоритми, побудовані на базі еліптичних кривих визначених у 2 вимірах. Але не існує алгоритмів, побудованих на еліптичних кривих, визначених у більшій кількості вимірів. Також не існує алгоритмів для проведення операцій суми і множення точки на число для загального випадку для кривих, визначених у n вимірах.

Збільшення порядку вимірів у яких визначена еліптична крива призведе до збільшення кількості точок у скінченному полі Галуа, що в свою чергу дасть можливість досягти більшого рівня криптостійкості за тієї ж довжини ключа. Або при використанні цього алгоритму, можна досягнути того ж рівня криптостійкості за меншої довжини ключа. А використання процесорних операцій над векторами дозволить проводити обчислення з тою ж швидкістю, що і над кривою, визначеною у двох вимірах.

З зростом потужності обчислювальних приладів з’являться ще одна проблема: потреба у постійному ускладненні користувацьких паролів з метою запобігання втручання зловмисників.

Для роботи в сучасній корпоративній інфраструктурі працівникам недостатньо використання тільки одного пароля. Кожен додаток типу ERP або CRM, системи управління базами даних, корпоративні програми, системи аутентифікації, програми-клієнти банків, програми для опрацювання бухгалтерського аудиту тощо зазвичай має свою систему захисту і аутентифікації, що вимагає створення для кожного такого додатку пароля. У таких випадках, існує два можливих варіанти створення паролів:

- використання одного пароля для кожного додатку,
- використання унікального пароля для кожного додатку.

Використання одного пароля небезпечне тим, що ця політика в рази погіршує захищеність даних від викрадення.Таким чином, якщо корпорація дбає про безпеку інформації і намагається уникнути викрадення даних, то вона зобов’язує працівників створювати унікальні паролі для кожного додатку. З року в рік кількість паролів, які повинен пам’ятати працівник збільшується а їх складність зростає. Для запобігання втручання зловмисників використовується ще одна міра захисту: постійна примусова зміна паролів через певний проміжок часу.

У цієї корпоративної політики є один суттєвий недолік. Працівник повинен пам’ятати велику кількість складних паролів, а отже зростає імовірність забування паролю працівником.

За оцінками компанії Rainbow Technologies, кожне звернення дослужби підтримки з проханням відновити дані через забутий пароль може коштувати до 37,50 доларів.

Використання стандартного парольного захисту має ще один суттєвий недолік. З дослідження Computer Security Institute отримано результат, що до 84% всіх випадків заволодіння інформацією зловмисниками в сучасних компаніях відбуваються через людський фактор: з вини непрофесійних,

непродуманих дій працівників та через вину недобросовісних працівників.

Для уникнення проблеми витоку інформації через людський фактор використовуються менеджери паролів. Менеджер паролів це додаток у функції якого входить зберігання у зашифрованому виді усіх паролів користувача і видача їх користувачу у відповідь на запит. Використовуючи менеджер паролів працівник не повинен запам’ятовувати усі паролі, достатньо запам’ятати пароль від менеджеру паролів. Таким чином, працівники не знатимуть паролі для аутентифікації до різних додатків, і не зможуть випадково чи навмисно повідомити їх зловмисникам.

Системи генерування та зберігання паролів можуть вирішити цю проблему. У випадку використання такої системи користувачу достатньо пам'ятати один пароль від програми. Всі інші паролі зберігатимуться у програмі, з можливістю їх легкого отримання користувачем.

1. ПОСТАНОВКА ЗАДАЧІ

Метою дисертації є створення системи аутентифікації з меншою необхідною довжиною ключа за рахунок збільшення кількості вимірів у яких визначена еліптична крива, та збереженням рівня криптостійкості.

Задачі:

- Дослідження переваг еліптичної кривої визначеної в n+1 вимірах над еліптичною кривою визначеною в n вимірах.
- Аналіз отриманих результатів.
- Реалізація алгоритму електронного цифрового підпису на базі еліптичних кривих визначених в n вимірах.
- Дослідження переваг алгоритму ЕЦП на базі еліптичних кривих визначених в n+1 вимірах над алгоритмом ЕЦП на базі еліптичних кривих визначених в n вимірах.
- Реалізація алгоритму генерування паролів

Об’єкт дослідження:

Система аутентифікації на базі еліптичних кривих.

Предмет дослідження:

Вплив кількості вимірів у яких визначена еліптична крива на криптостійкість ЕЦП.

2. ОГЛЯД ІСНУЮЧОГО СТАНУ ПРОБЛЕМНОЇ ОБЛАСТІ

Системи аутентифікації на сьогодні використовують асиметричну криптографію, оскільки цей розділ криптографії крім шифрування дає можливість аутентифікації, перевірки цілісності даних та ідентифікації. Першим протоколом асиметричної криптографії є протокол RSA. Це алгоритм який може використовуватися і для шифрування і для реалізації електронного цифрового підпису. Він реалізований на базі скінченного поля Галуа над цілими числами.

Асиметричні алгоритми працюють наступним чином. Спочатку генерується пара ключів: публічний і секретний. Публічний ключ знаходиться у вільному доступі у спеціальних таблицях компаній, які мають відповідний сертифікат. А секретний ключ знаходиться тільки у власника пари ключів. Його розповсюдження скомпрометує валідність шифру.

Шифрування проводиться використовуючи публічний ключ особи, якій відправляється повідомлення. Тепер розшифрувати його можна тільки використавши секретний ключ.

RSA може використовуватися не тільки для шифрування, але й для цифрового підпису. Для підпису потрібно використати секретний ключ:

$$s = m^d mod\ n$$

Тепер використавши публічний ключ можна отримати початкове повідомлення:

$$\mathrm{m} = \mathrm{s}^{\mathrm{e}} \mathrm{mod\ n}$$

Таким чином отримавши повідомлення і його підпис, а потім провівши дешифрування за допомогою публічного ключа користувача можна переконатися, що підписати його міг тільки він.

У алгоритму є свої переваги: він тестувався протягом багатьох років, і не було знайдено методів, які би суттєво зменшували криптостійкість алгоритму.

Але у порівнянні з асиметричними алгоритмами на базі еліптичних кривих у скінченному полі алгоритм на базі скінченного поля на просторі цілих чисел має такі недоліки: для його реалізації потрібно більший ключ і відповідно більші затрати часу.

2.1. Протоколи для забезпечення аутентифікації на базі еліптичних кривих

У 1986 році з’явились алгоритми асиметричної криптографії на базі точок еліптичної кривої у скінченному полі Галуа.

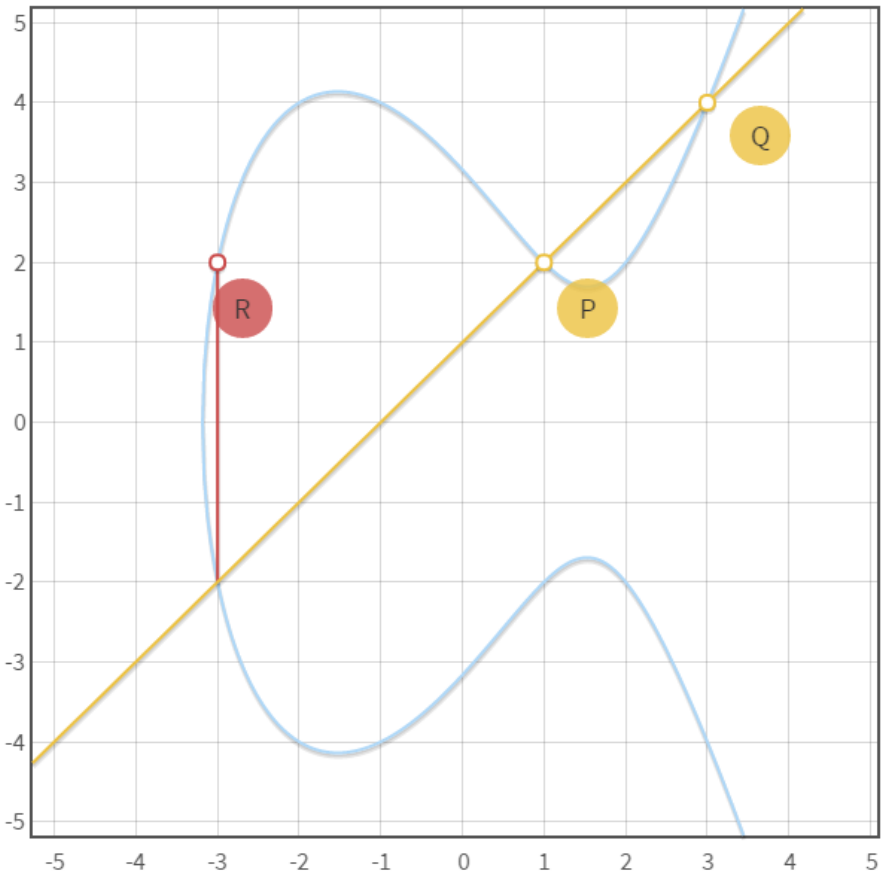


Рисунок 2.1 – Еліптична крива і графічне зображення операції суми

На сьогоднішній день у різних країнах існують свої протоколи забезпечення аутентифікації на базі еліптичних кривих:

- ECDSA
- ГОСТ 34.10-2012
- ДСТУ 4145-2002

2.1.1. Алгоритм ЕЦП на базі еліптичних кривих ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) — перший алгоритм шифрування з відкритим ключем на базі точок еліптичної кривої в скінченному полу Галуа.

Цей алгоритм був прийнятий стандартом ISO в 1998 році,в 1999 стандартом ANSI, також в 2000 році — в IEEE та NIST.

Стандартом запропоновано п’ять кривих різного порядку, які вважаються достатнього рівня стійкості для того, щоб не зменшити криптостійкість алгоритму.

Головними недоліками еліптичної криптографії є те, що відсутність субекспоненціного вирішення проблеми дискретного логарифму в точках еліптичної кривої не доведена, і коли знайдеться такий алгоритм, то усі переваги еліптичної криптографії зникнуть, і залишаться тільки недоліки у виді важкості алгоритму, та відносно більших затрат часу на довжину ключа при реалізації підпису.

2.1.2. Алгоритм ЕЦП на базі еліптичних кривих ГОСТ 34.10-2012

ГОСТ Р 34.10-2012 та ГОСТ Р 34.10-2001 аналог ECDSA в країнах СНД. Стійкість алгоритму визначається складністю проблеми обчислення дискретного логарифму в группі точок еліптичної кривої, але на відміну від

стандарту ANSI в ГОСТ Р 34.10-2012 та ГОСТ Р 34.10-2001 додаткову стійкість дає хеш-функція. Для хеш-функцій використовуються стандарти ГОСТ Р 34.11-2012 та ГОСТ Р 34.11-94 відповідно.

Стандарт 2012 року абсолютно повторює стандарт 2001 року, за винятком збільшення довжини мінімального порядку скінченного поля у якому визначена еліптична крива з 256 біт до 512

Алгоритм передбачав додавання до повідомлення цифрового підпису розміром в 512 або 1024 біти, а також додаткової інформації, такої як дати підпису, тощо.

В даному алгоритмі відсутні рекомендовані криві, їх генерування визначається в кожній окремій системі індивідуально.

2.1.3. Алгоритм ЕЦП на базі еліптичних кривих ДСТУ 4145-2002

Стандарт ДСТУ 4145-2002 – український аналог стандарту ECDSA. Мало чим відрізняється від російського варіанту стандарту. Затверджений 28 грудня 2002 року наказом Державного комітету України з питань технічного регулювання та споживчої політики. З того часу сертифікат не зазнав змін.

В цьому стандарті також визначався алгоритм та мінімальні критерії криптостійкості. Він базувався на ключі не менше 1024 біт, і був дійсний до 31 грудня 2010 року.

Стандартом як і в російському аналогу відсутні рекомендовані стандартом криві, і вони визначаються індивідуально для кожної системи.

2.1.4. Порівняльний аналіз алгоритмів цифрового підпису

Для того, що порівняти наведені вище стандарти між собою основні дані винесені до таблиці 2.1.

Таблиця 2.1 – Порівняння стандартів різних країн

Назва алгоритму	Довжина ключа(біт)	Рік прийняття стандартом
ECDSA	160	1998
ГОСТ 34.10-2012	256, 512	2001, 2012
ДСТУ 4145-2002	512	2002

Для того, щоб довести набагато більшу криптостійкість алгоритмів, побудованих на базі еліптичних кривих відносно алгоритмів на базі цілих чисел, наведено дані в таблиці 2.2 про довжину ключа, необхідну для різних алгоритмів, для забезпечення необхідного рівня стійкості.

Таблиця 2.2 – Порівняння довжини ключа для алгоритмів

Криптостійкість(bit)	RSA довжина публічного ключа (bit)	ECDSA довжина публічного ключа (bit)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Для наглядності дані з таблиці 2.2 оформлені у вигляді графіку на рисунку 2.2

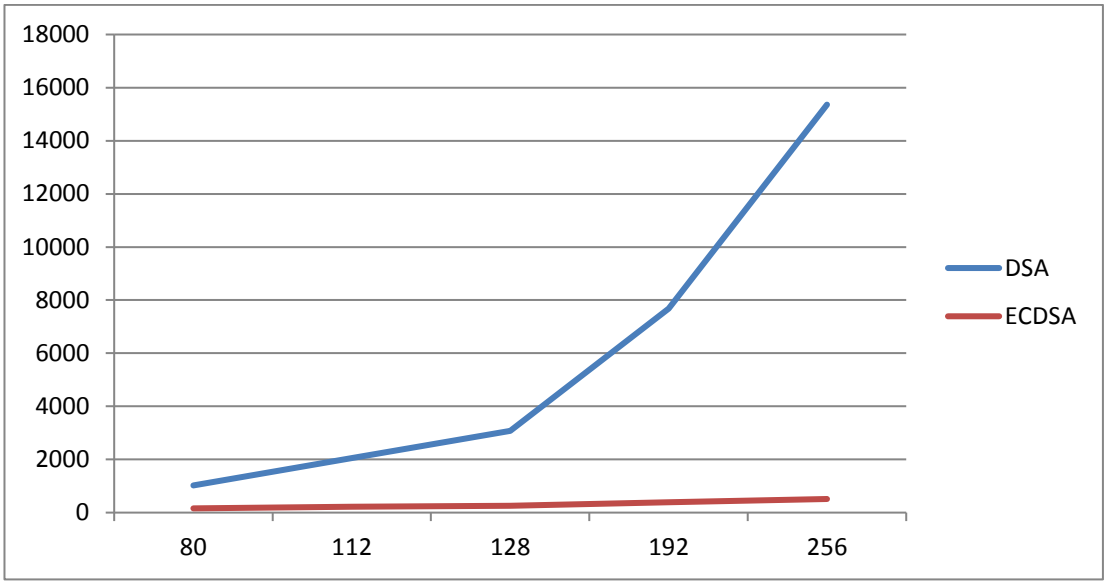


Рисунок 2.2 – Графіки порівняння необхідних довжин ключів для різних алгоритмів

2.1.5. Алгоритм реалізації ЕЦП на базі еліптичних кривих

Якщо Аліса намагається довести Бобу що деяка інформація належить їй то вона повинна зробити наступне:

1. Обрати випадкове число

$$k, 1 \leq k \leq n - 1,$$

де n – порядок базової точки.

2. Обчислити

$$kG = (x_1, y_1),$$

та провести конвертування x до $\bar{x}$

3. Обчислити $r = \bar{x} \pmod n$. Якщо $r = 0$ то повторити обчислення починаючи з кроку 1.

4. Обчислити

$$k^{-1} \pmod{n},$$

де k^{-1} – протилежне по модулю число, яке:

$$k^{-1}k \pmod{n} = 1$$

5. Обчислити SHA-1 – хеш-суму m

$$SHA(m),$$

та проконвертувавши, отримати число m

6. Обчислити

$$s = k^{-1}(e + K_{priv}r)(\mathrm{mod}\ n)$$

Якщо $s = 0$ – повернутися до кроку 1

7. Результатом підпису повідомлення m буде пара (r, s)

Тепер Аліса відправляє Бобу пару (r, s) та свою інформацію. У Боба для перевірки того, що саме Аліса відправляє ці дані потрібно щоб була пара (r, s), саме повідомлення, а також публічний ключ Аліси, який він може отримати або безпосередньо від Аліси попередньо, або в списку публічних ключів тої системи генерування ключів, де вони були створені Алісою. Тепер для перевірки підпису Боб повинен:

1. Запевнитися, що r та s – числа в інтервалі $[1, n-1]$
2. Обчислити SHA-1(m) та отримати обернене число по модулю e
3. Обчислити

$$w = s^{-1} \pmod{n}$$

4. Обчислити

$$u_1 = ew \pmod{n},$$

Та

$$u_2 = rw \pmod{n}$$

5. Обчислити

$$X = u_1 G + u_2 K_{pub}$$

6. Якщо $X = 0$, підпис скомпрометовано, інакше, проконвертувати x координату точки X в число $\overline{x_1}$, та обчислити

$$v = \overline{x_1} \pmod{n}$$

7. Підтвердити підпис, якщо

$$v = r$$

2.2.Методи аутентифікації

Кожна система аутентифікафії використовує методи які можна поділити на 4 групи:

- Знання секретної інформації
- Використання унікального предмета

– Використання біометричних параметрів людини

– Інші інформація про користувача

Знання секретної інформації включає в себе такі методи захисту як використання паролю, відповідь на секретне запитання, яке разом з відповіддю було обране раніше, коли особа була аутентифікована (наприклад написання заяви для отримання розрахункової карти в банку, коли аутентифікація особи проводиться через дані паспорту). Головні переваги цього методу простота і звичність. Через ці переваги цей метод аутентифікації є найпопулярнішим. Він використовується для аутентифікації на електронні ресурси, при входженні в операційну систему на персональному комп'ютері, при отриманні даних з банку тощо. При правильному використанні цей метод дає прийнятний рівень безпеки для більшості повсякденних справ. Проте через велику кількість уразливих місць цей метод можна вважати найменш безпечним методом аутентифікації. Парольний захист недостатній для операцій з важливими даними, наприклад при грошових операціях, проте можливий як одна з частин багатофакторної аутентифікації.

Поширена практика сумісного використання декількох з перерахованих вище механізмів – у таких випадках кажуть про багатофакторну аутентифікацію.

Існує ряд заходів для підвищення надійності захисту за допомогою знання секретної інформації:

– Встановлення вимог до розміру, форми, вмісту паролю. Цей захід підвищення надійності часто використовується на електронних ресурсах, де до паролю є вимоги – мінімальний розмір, вміст принаймні одної літери і цифри, вміст принаймні одної великої літери.

– Встановлення терміну дії паролю. Захід використовується в більшості систем управління базами даних, на підприємствах, для аутентифікації працівників тощо.

– Обмеження доступу до файла паролів. Захід, яким, серед інших,

користуються програми клієнт-банкінгу.

– Використання програм-генераторів. Захід, який використовується для неможливості використання таблиць, які містять найчастіше використовувані паролі.

Програми генератори паролів є декількох видів:

– програма, на вхід якої потрібно написати якесь слово або декілька слів, які будуть основою пароля, тоді на виході програма перетворить деякі літери алфавіту на символи, які легко запам’ятати, але вони сильно збільшать час потрібний для знаходження паролю методом брутфорсу, така програма наведена на рисунку 2.3.

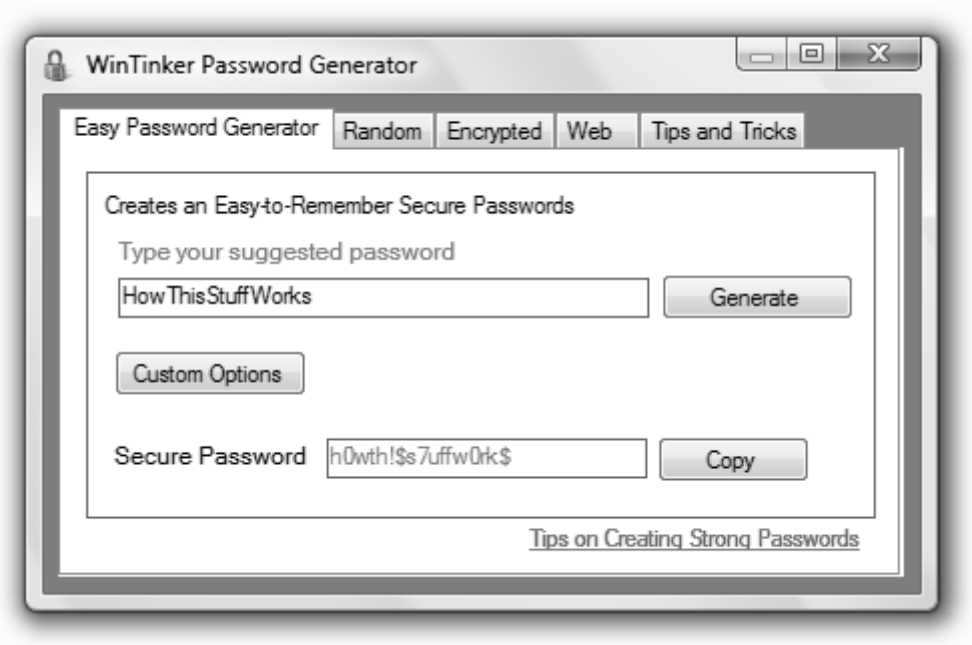


Рисунок 2.3. – Вигляд програми генератора пароля

– програма, для якої потрібно задати розмір пароля, присутність чи відсутність великих літер, цифр тощо. В результаті, отриманий пароль буде важко запам’ятати, але його майже неможливо буде знайти методом підбору. Програму такого виду можна побачити на рисунку 2.4:

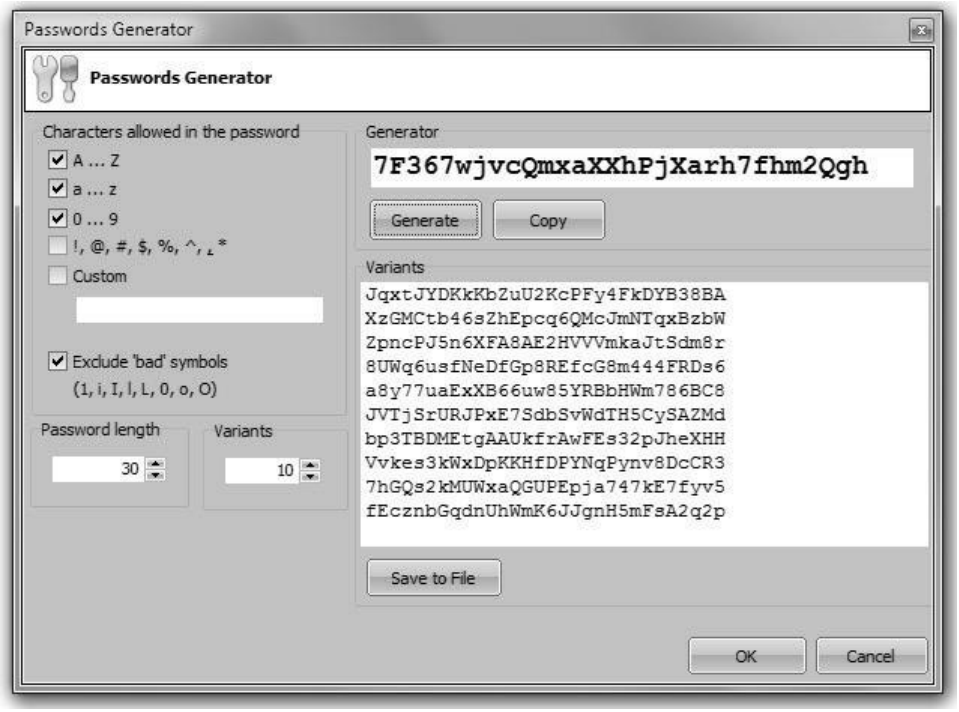


Рисунок 2.4. – програма генератор випадкового паролю

Навіть з використанням цих заходів для парольного захисту є декілька типів загроз безпеки методу:

– Випадкове або навмисне розголошення паролю власником.

– Отримання паролю злочинцем за допомогою соціальної інженерії

– Втручання у функціонування програмних компонентів: впровадження зловмисного програмного забезпечення, використання програмних помилок, виведення з ладу системи.

Перераховані загрози в більшості пов'язані з наявністю людського фактору. Найбільшою проблемою систем є те що її стійкість залежить від людини. Для вирішення цієї проблеми використовується так званий менеджер паролів, за допомогою цього програмного застосування не потрібно запам'ятовувати усі паролі а також є можливість створювати випадково згенеровані паролі для кожного нового ресурсу. У таких системах є декілька методів зберігання паролів: у відкритому вигляді, у вигляді хешування, зашифрованими за деяким ключем.

Якщо перший метод не дає ніякого захисту і будь-яка злочинна програма

матиме змогу отримати доступ до паролів, то два інші способи мають деякі особливості.

Хешування (використання незворотної хешфункції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору паролів по словнику у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати неспівпадання значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність згорток у випадку, якщо два користувачі вибирають однакові паролі.

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів. Перерахуємо деякі можливі варіанти: ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження; ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску; ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску.

Найбезпечніше зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при їх комбінації.

Використання унікального предмета. Унікальним предметом у даному випадку може бути будь-який фізичний пристрій-ідентифікатор.

Призначення таких пристроїв:

– Аутентифікація при доступі до захищених об'єктів

На рисунку 2.5 можна помітити спеціальний ключ-картку, за допомогою якої працівники проходять аутентифікацію при приході на роботу.

Рисунок 2.5. – ключ-карта

- Зберігання закритих ключів, цифрових сертифікатів тощо
- Апаратне виконання криптографічних алгоритмів

Для апаратного виконання криптографічних алгоритмів використовуються спеціальні USB-токени, приклад якого наведений на рисунку 2.6.

Рисунок 2.6. – USB – токен.

Переваги:

- Відсутність людського фактору
- Безпечне зберігання секретної інформації
- У порівнянні з парольним захистом набагато вищий рівень стійкості

Недоліки:

- При втраті пристрою аутентифікація стає неможливою
- Неможливість використання в мережі інтернет

Біометрична аутентифікація – спосіб аутентифікації особи за допомогою визначення специфічних біологічних параметрів. До таких біологічних параметрів відносять:

- Відбиток пальців

Найчастіше використовуваний метод. Для зчитування відбитків пальців використовуються спеціальні сканери. Раніше в докомп'ютерну еру порівняння відбитків пальців використовувалися тільки для доведення причетності вини злочинця, якщо знаходилося співпадіння. На сьогодні сканери відбитків пальців часто використовуються для розблокування телефонів, ноутбуків, планшетів. На рисунку 2.7 можна помітити спеціальний сканер, який вставляється через USB порт.

Рисунок 2.7. – сканер відбитку пальців.

– Малюнок сітківки

На сьогоднішній день все частіше використовуваний метод для розблокування телефонів та інших пристроїв. Раніше використовувався тільки в спеціальних захищених приміщеннях. Це пояснюється тим, що прилад для сканування сітківки повинен бути досить високої роздільної здатності, і мав велику собівартість, та з часом технологія подешевшала, і стало можливим її повсякденне використання. На рисунку 2.8. можна помітити сканер сітківки реалізований під веб камеру, яку можна використовувати для аутентифікації в персональному комп’ютері.

Рисунок 2.8. – сканер сітківки ока

– Голос

На сьогодні технологія аутентифікації по голосу часто використовується при використанні віртуальних помічників чи розумних домів. У цьому випадку не настільки важлива безпека, як швидке і просте визначення просьби людини. На рисунку 2.9 зображений пристрій віртуального помічника Alexa.

Рисунок 2.9. – домашній помічник Alexa

– Почерк

Почерк часто використовувався для аутентифікації на документах, у вигляді звичайного підпису. Цей метод став популярним через свою простоту, але недоліком є легка можливість підробити підпис. На рисунку 2.10 зображено пристрій для аутентифікації за допомогою підпису.

Рисунок 2.10. – пристрій аутентифікації за допомогою підпису

– Термограма обличчя

Метод на сьогодні не має велику популярність через низьку якість аутентифікації, але на відміну від сканування контурів обличчя, яке тепер популярне на сучасних телефонах, термограма обличчя може розрізняти близнюків. Система аутентифікації може набути велику популярність, після збільшення точності до потрібного рівня, оскільки для реалізації достатньо з апаратної частини тільки інфрачервону камеру.

– Унікальність вушної раковини

Метод аутентифікації який на сьогодні не набув великої популярності, хоча унікальність вушної раковини більша ніж у всіх інших варіантів аутентифікації за фізичною унікальністю. Невелика розповсюдженість пояснюється важкістю реалізації простого алгоритму для визначення вушної раковини. Існує два методи аутентифікації вушної раковини: на основі

трьохвимірної моделі і на основі відбитку вуха. Метод з трьохвимірною моделлю вуха важкий у реалізації, оскільки для нього у пристрої потрібно щонайменше дві камери, які знаходяться на певному відстані одна від одної. Метод відбитку вуха досить легко реалізований, можливий для використання на мобільних телефонах, але унікальність відбитку вушної раковини не доведена.

При великій кількості різних можливих параметрів усі вони зводяться до однакового методу розпізнавання і аутентифікації на базі знайдення співпадіння у базі даних користувачів.

Усі біологічні ознаки поділяються на дві групи:

– Статичні
– Динамічні

До статичних ознак відносять такі які практично не змінюються з часом починаючи від народження людини і все її життя.

Динамічні ознаки це такі, які побудовані на особливостях підсвідомих рухів

Перевагою біометричної аутентифікації є неможливість або майже неможливість втрати засобу аутентифікації, а недоліком такого методу аутентифікації є неможливість використання його програмою.

Прикладом інформації асоційованої з користувачем можуть бути координати користувача, визначені за допомогою GPS. Цей підхід навряд чи може бути використаний як єдиний механізм аутентифікації, проте цілком допустимо його використання як додаткового елементу захисту

На сьогоднішній день для досягнення хорошого рівня захисту при проведенні аутентифікації використовується метод двофакторної аутентифікації, або метод багатофакторної аутентифікації.

Зазвичай першою частиною двофакторної аутентифікації використовують парольний захист. Використавши менеджер паролів можна досягти того, що злочинець отримавши незаконним шляхом пароль користувача зможе отримати доступ тільки до одного ресурсу чи програми. Але з певною імовірністю він може отримати доступ до важливих документів чи операцій.

Для уникнення таких ситуацій використовується двофакторна аутентифікація, при якій отримати пароль буде недостатньо.

Двофакторна аутентифікація використовує методи з двох груп наведених вище, в рідших випадках три або чотири.

Використання лише паролю або відбитку для відстеження доступу до своїх облікових записів, визначає однофакторну аутентифікацію. В деяких випадках двофакторна аутентифікація використовує методи з одної групи, тоді цей метод аутентифікації є лише замаскований під двофакторну аутентифікацію одно факторний.

Найчастіше під двофакторною аутентифікацією розуміють два методи: парольний захист і секретний код, отриманий в смс на телефонний номер. Насправді цей метод використовує в обидва фактори групу методів з секретними даними. Користувач не володіє номером телефону, його власником є компанія телефонного оператору. Зловмисник може отримати доступ до смс користувача за допомогою соціальної інженерії.

3. ІСНУЮЧІ СИСТЕМИ АУТЕНТИФІКАЦІЇ

3.1.Система аутентифікації «ПСКЗИ ШИПКА»

Система аутентифікації «ПСКЗИ ШИПКА» реалізує всю систему аутентифікації і захисту через апаратний пристрій будь-якого типу:

- TM-ідентифікатори DS-1992 року,
- DS-1993, DS-1996 року,
- USB-ключі виду eToken,
- JaCarta «ACOSxx» ,
- USB-пристрої,
- смарт-карти,
- «ESMART Token xx»

На рисунку 3.1. зображений USB пристрій на якому реалізовано аутентифікацію.

Рисунок 3.1. – Персональний засіб аутентифікації

Крім того, для реалізації механізму апаратної ідентифікації в «ОКБ САПР» розроблений ПАК «ПИ ШИПКА».

Програмно-апаратний комплекс «ПИ ШИПКА» включає в себе:

- апаратну базу - USB-пристрій;
- вбудовуване програмне забезпечення;

– програмну надбудову - спеціальне програмне забезпечення.

Нижче, на рисунку 3.1 зображено вигляд програмного забезпечення.

Рисунок 3.1 – Зовнішній вигляд програми «ПСКЗИ ШИПКА»

Для використання програмно апаратного комплексу «ПИ ШИПКА» є ряд мінімальних вимог для системи:

– Персональний комп’ютер з наявністю USB роз’єму;

– Установлена операційна система сімейства Windows або Linux;

Ключові функції

Реалізація аутентифікації за допомогою зовнішнього пристрою.

Можливість реалізації двофакторної аутентифікації, при одному зовнішньому факторі.

3.2.JaCarta WebPass

JaCarta WebPass це програмно апаратний комплекс, який реалізує наступні функції:

– генерування паролів на пристрої

– чотири алгоритми генерування паролю

– заповнення паролів у необхідні поля
– створення одноразового паролю
– використання до трьох паролів

Такий пристрій вирішує наступні проблеми:

– проблема забування паролю,
– проблема отримання паролю методами соціальної інженерії,
– проблема генерування працівниками занадто слабких паролей.

На рисунку 3.3 зображено вигляд USB-токену JaCarta WebPass

Рисунок 3.3 – Зовнішній вигляд USB-токену JaCarta WebPass

Таки пристрій має ряд функцій, які можна реалізувати для трьох різних програм де потрібно реалізувати аутентифікацію. Для кожного з трьох різних варіантів реалізації певної функції можна отримати результат або одноразовим або подвійним або тривалим натисканням кнопки, яка присутня на пристрої.

На рисунку 3.4 зображено користувацьке вікно консолі управління токенами.

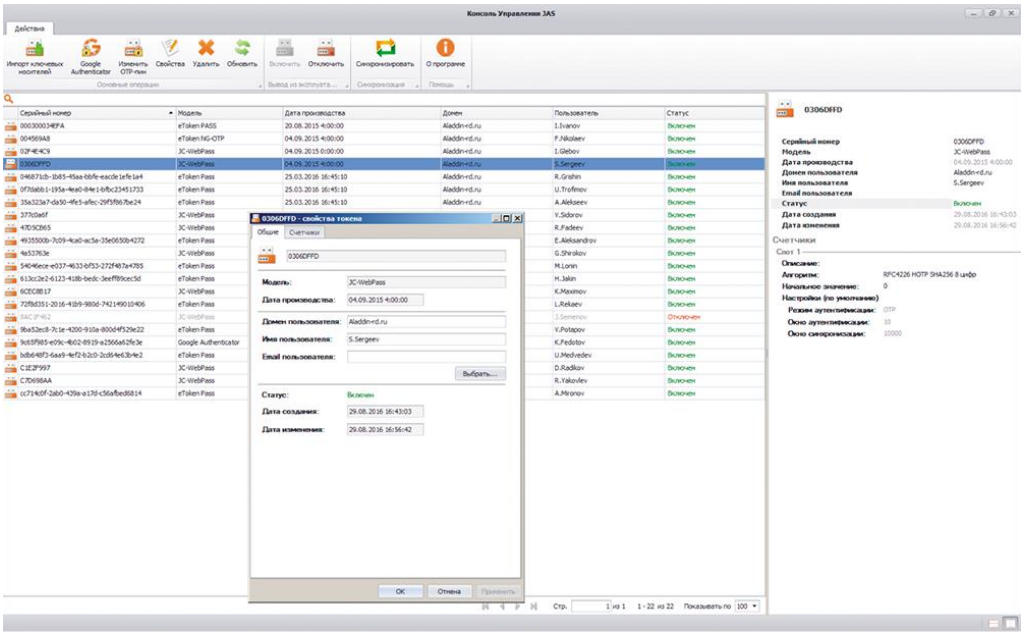


Рисунок 3.4 – Користувацьке вікно консолі управління токенами

3.3.ZShell

Zshell - Система аутентифікації користувачів

Zshell – програма менеджер паролів. Установивши систему інтегровано як службу каталогів Active Directory кожен користувач зможн нею користуватися. Програма має наступні функції:

- зберігання необмеженої кількості паролей,
- заповнення паролю у потрібні вікна,
- налаштування складності паролів,
- захист записаних паролів від зловмисників.

Таким чином ця система аутентифікації користувачів вирішує одразу декілька проблем:

- проблему отримання зловмисниками паролю від працівників методами соціальної інженерії,
- проблему забування паролів,
- проблему створення працівниками слабких і однакових паролів через неможливість запам’ятання більшої кількості символів.

Сумісність:

Система Zshell сумісна з усіма типами Win32 додатків, що використовують для аутентифікації користувачів діалогові вікна. Система Zshell протестована на сумісність з багатьма додатками, серед яких:

- Microsoft Office,
- Outlook Express,
- 1С: Підприємство,
- F-Secure SSH Client

3.4.Порівняння систем аутентифікації

Для порівняння описаних систем аутентифікації було розроблено таблицю 3.1.

Таблиця 3.1. – порівняльна характеристика функцій програми

Функції систем	LastPass	JaCarta WebPass	ZShell
Створення пари ключів	Відсутнє	Присутнє	Присутнє
Можливість застосування смарт-карт	Відсутня	Присутня	Відсутня
Можливість використання через мережу інтернет	Присутня	Відсутня	Присутня

Можливість застосування на різних ОС	Присутня	Присутня	Відсутня
Менеджер паролів	Присутній	Відсутній	Присутній
Двофакторна аутентифікація	Присутня	Присутня	Присутня

4. РОЗРОБКА БАГАТОВИМІРНОЇ ЕЛІПТИЧНОЇ КРИВОЇ

На сьогоднішній день в криптографії використовуються тільки еліптичні криві визначені у двох вимірах.

Така крива у загальному виді має вигляд:

$$y^2 = x^3 + ax^2 + bx + c$$

Але найчастіше для зручності обчислень еліптичну криву записують наступним чином:

$$y^2 = f(x); f(x) = x^3 + ax^2 + bx + c,$$

де a, b, c дійсні числа.

В усіх стандартах де використовується еліптична криптографія використаний частковий випадок де $a = 0$:

$$y^2 = f(x); f(x) = x^3 + bx + c$$

На рисунку 4.1 зображена еліптична крива, визначена у двох вимірах.

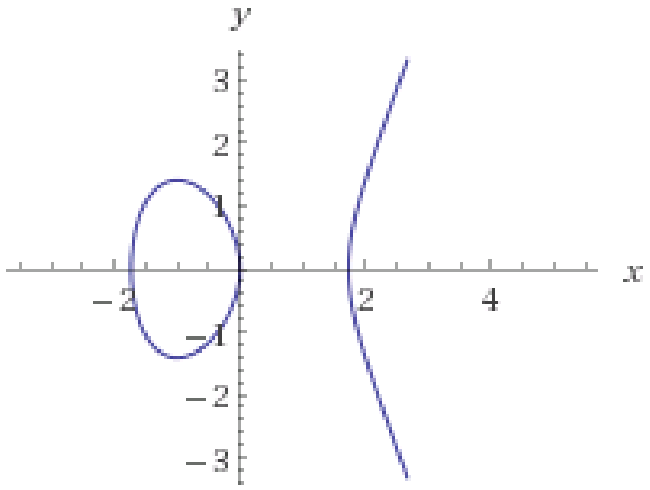


Рисунок.4.1 – Приклад кривої визначеної у двох вимірах

Сингулярні еліптичні криві

Перенесемо праву частину рівняння (4.1) вліво:

$$F(x, y) = y^2 - f(x) = 0$$

Тепер, взявши часткові похідні змінних отримаємо:

$$\frac{\partial F}{\partial x} = -f'(x); \frac{\partial F}{\partial y} = 2y;$$

Якщо існує точка (x_0, y_0) де часткові похідні прямують до нуля, то $y_0 = 0$, многочлени $f'(x)$ та $f(x)$ мають однаковий корінь x_0, а точка (x_0, y_0) називається сингулярною точкою. Крива у якої є сингулярна точка, називається сингулярною кривою.

В залежності від того, чи $f(x)$ має подвоєний, чи потроєний корінь, існує два можливих варіанта сингулярної кривої.

Для подвоєного кореня типовим є рівняння виду:

$$f(x) = (x + a)^2(x + b)$$

Приклад:

$$y^2 = x^2(x + 3)$$

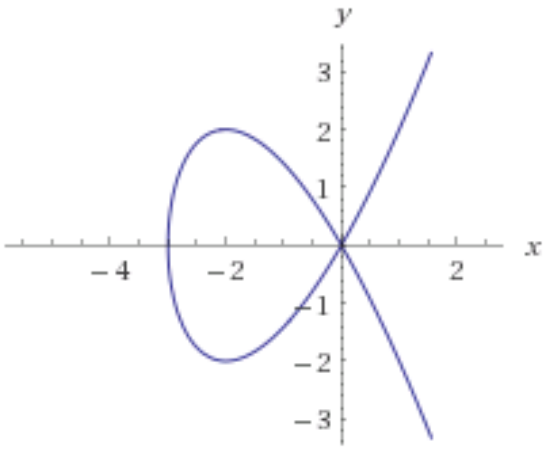


Рисунок.4.2 – Приклад сингулярної кривої з подвоєним коренем

На Рис 4.2 точка (0,0) є сингулярною.

Для кривої з потроєним коренем типовим рівнянням є:

$$f(x) = (x + a)^3$$

Приклад:

$$y^2 = (x + 3)^3$$

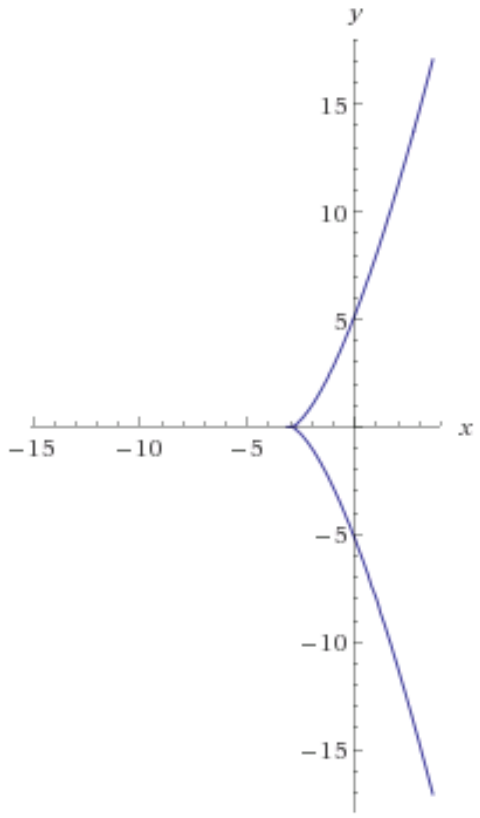


Рисунок.4.3 – Сингулярна крива з потроєним коренем

На Рис.4.3 точка $(-3,0)$ є сингулярною точкою.

Оскільки операція суми для точок еліптичної кривої виходить з геометричного доведення, то для кожної точки повинна існувати єдина визначена дотична. Для сингулярної точки існує безліч похідних, тому криптостійкість суттєво зменшиться.

Для таких кривих існує субекспоненційне рішення проблеми дискретного логарифму у скінченному полі а отже криптостійкість таких кривих можна прирівняти до асиметричної криптографії в скінченному полі Галуа над цілими числами.

Сингулярність для еліптичних кривих визначених у більшій кількості вимірів має такі самі властивості з відмінністю у тому, що для зменшення криптостійкості достатня наявність сингулярності в одному вимірі.

Суперсингулярні еліптичні криві

Для еліптичної криптографії важливим поняттям є порядок еліптичної кривої, який вказує кількість точок кривої над скінченним полем.

Теорема Хассе:

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Де N – кількість точок кривої;

GF(q) – скінченне поле Галуа;

q – кількість елементів поля GF.

Перетворивши нерівність, отримаємо кількість точок кривої:

$$E_q(a, b) = q + 1 - t;\ |t| \leq \sqrt{q}$$

t – слід відображення Фробеніуса–

Еліптична крива називається суперсингулярною тоді, коли для неї справедлива рівність:

$$t\ mod\ q = 0$$

Суперсингулярні криві у криптостійкості прирівнюються до сингулярних.

Аномальні еліптичні криві

Як було сказано раніше, для визначення кількості точок еліптичної кривої над скінченни полем використовують формулу:

$$E_q(a, b) = q + 1 - t;\ |t| \leq \sqrt{q}$$

Аномальною еліптичною кривою називають таку криву для якої

$$E_q(a, b) = q$$

тобто:

$$t = 1$$

У цьому випадку існує навіть швидший алгоритм для вирушення проблеми дискретного логарифму у скінченному полі, тому використання таких кривих небажане.

Загальний вигляд еліптичної кривої, визначеної в n вимірах

Запишемо еліптичну криву у канонічній формі:

$$y^2 = X^3 + AX^2 + BX + C,$$

де $X = [x_1 \quad x_2 \quad \cdots \quad x_n]$,
$A = [a_1 \quad a_2 \quad \cdots \quad a_n]$,
$B = [b_1 \quad b_2 \quad \cdots \quad b_n]$,
$C = [c_1 \quad c_2 \quad \cdots \quad c_n]$,
n – кількість вимірів.

Приймемо $A = 0$, та запишемо рівняння у зручній для обчислення формі та з значеннями параметрів, які будуть використовуватися далі:

$$y^2 = f(X); f(X) = X^3 + BX + C$$

де $X = [x_1 \quad x_2]$,
$B = [-1 \quad -2]$,
$C = [1 \quad 0]$,

Ця крива у області дійсних чисел має наступний вигляд:

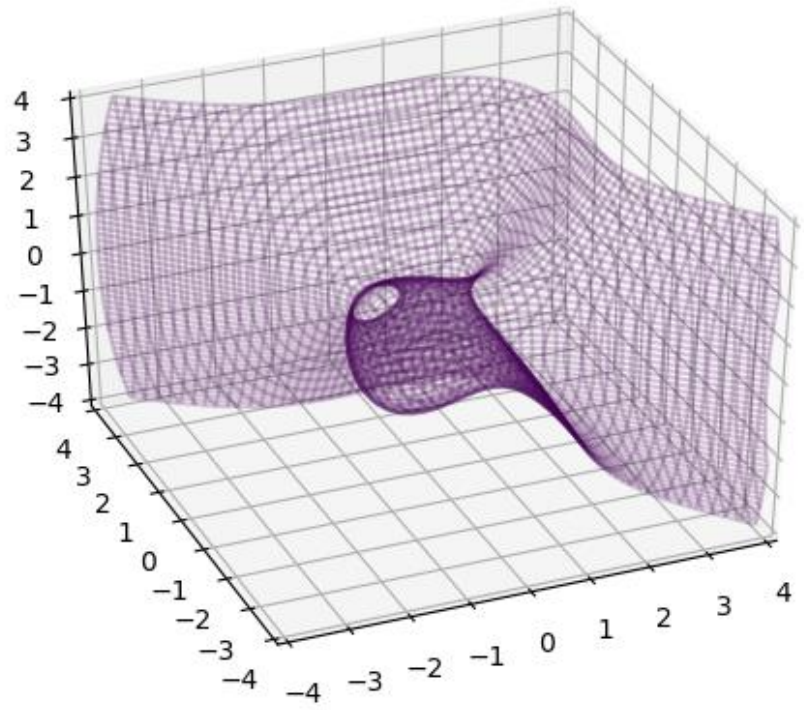


Рис.4.4 – Еліптична крива, визначена у трьох вимірах

Еліптична крива, визначена в n вимірах, в скінченному полі Галуа

У полі Галуа еліптична крива матиме вигляд скінченного набору точок. Для визначення цих точок скористаємося наступним алгоритмом:

1. Для кожного елементу декартового добутку $\boldsymbol{x_1 \times x_2 \times \ldots \times x_n}$ обчислимо $\boldsymbol{y^2}$ з формули:

$$y^2 = f(X); f(X) = (X^3 + BX + C)\ mod\ p\ ,$$

де $\boldsymbol{p}$ – порядок скінченного поля

2. Для всіх $\boldsymbol{y \in [0, p-1]}$ визначити чи вони будуть квадратичними лишками по модулю $\boldsymbol{p}$.

В результаті рівняння матиме наступний вигляд у скінченному полі порядку $\boldsymbol{p = 17}$:

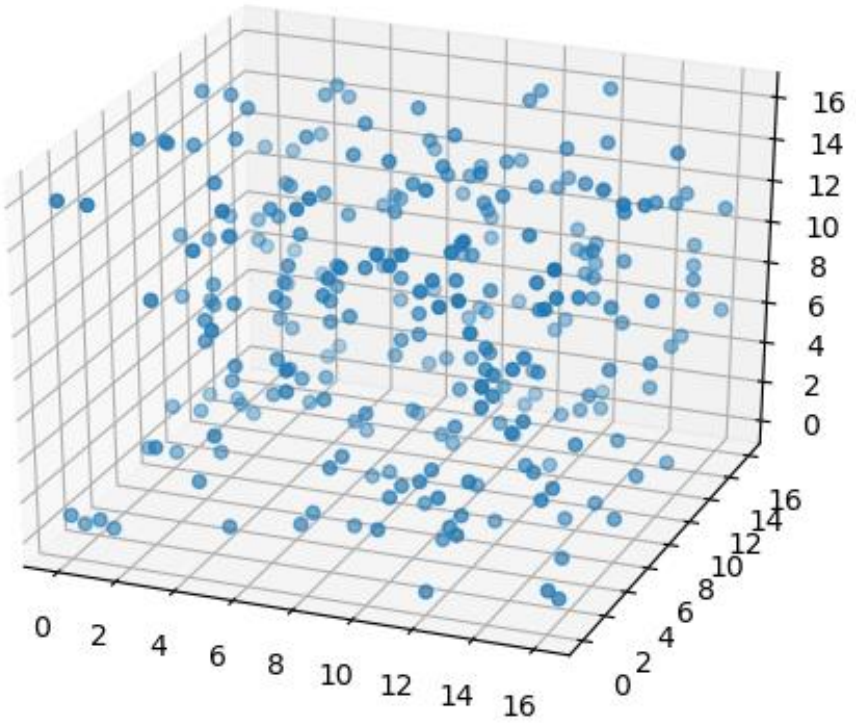


Рис.4.5 – Еліптична крива, визначена у трьох вимірах в скінченному полі

Дана крива в полі порядку $\boldsymbol{p = 17}$ створює групу з 272 точок. Для порівняння крива $\boldsymbol{y^2 \, mod \, 17 = x^3 - 1x + 1 \, mod \, 17}$ яка визначена у двох вимірах у скінченному полі такого порядку створюватиме групу з 13 точок

Визначення порядку еліптичної кривої

Крім того, що порядок кривої визначає її приналежність до суперсингулярних чи аномальних, кількість раціональних точок над скінченним полем є ще і важливим параметром для визначення стійкості.

Процес вибору кривої можна записати наступним чином:

1. Вибір коефіцієнтів, що описують рівняння кривої;
2. Визначення порядку кривої;
3. Порівняння отриманих результатів з необхідними

Для визначення порядку кривої існує декілька алгоритмів:

- Алгоритм Шуфа. Найбільш розповсюджений, але має ряд недоліків: досить високу обчислювальну складність: $\boldsymbol{O(log^6 q)}$, також алгоритм використовує складні математичні методи.

– Метод комплексного множення. Дозволяє знайти криві з заданим порядком. Працює набагато ефективніше у порівнянні з алгоритмом Шуфа, але не універсальний.

Сума точок еліптичної кривої

Оскільки на сьогоднішній день використовується тільки еліптична криптографія з кривими, визначеними у двох вимірах, то і операція суми точок кривої визначена тільки у кривих у двох вимірах. На основі цієї операції було розроблено вигляд операції суми для точок кривої визначеної у n вимірах.

Візьмемо еліптичну криву визначену у двох вимірах

$$\boldsymbol{y^2 = f(x); f(x) = x^3 + ax + b}$$

Нехай існують точки:

$$\boldsymbol{P, Q \in f(x)}$$

Тоді суму $\boldsymbol{P + Q = R}$ можна визначити як на рисунку:

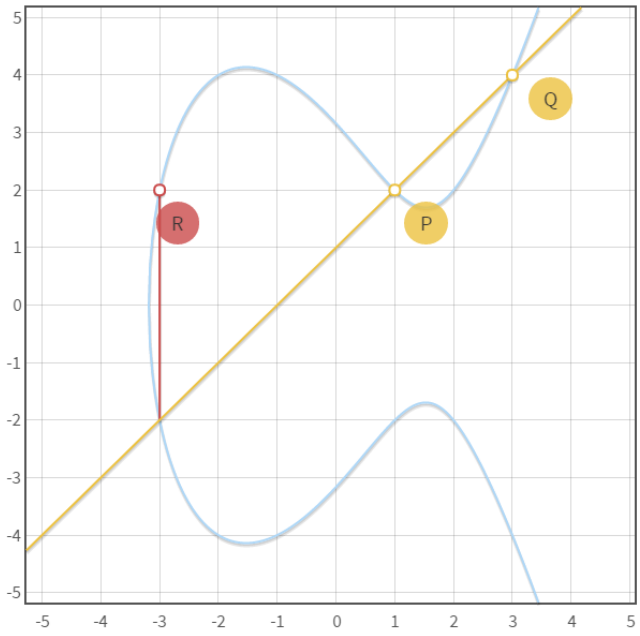


Рисунок 4.6 – Сума точок еліптичної кривої

На рисунку 4.6. операція суми проводиться на кривій:

$$\boldsymbol{y^2 = x^3 - 7x + 10}$$

Точок:

$$\boldsymbol{P(1,2); Q(3,4),}$$
$$\boldsymbol{P + Q = R,}$$
$$\boldsymbol{R(-3,2)}$$

На основі цього доведення можна отримати систему:

$$\begin{cases} \boldsymbol{x = S^2 - x_1 - x_2,} \\ \boldsymbol{y = -y_1 + S(x_1 - x),} \\ \boldsymbol{S = \dfrac{y_1 - y_2}{x_1 - x_2}} \end{cases}$$

Тепер, для загального випадку, коли еліптична крива визначена у n вимірах, запишемо попереднє рівняння:

$$\begin{cases} \boldsymbol{X = S^2 - X_1 - X_2,} \\ \boldsymbol{y = -y_1 + S(X_1 - X),} \\ \boldsymbol{S = \dfrac{y_1 - y_2}{X_1 - X_2}} \end{cases}$$

де $X = [x_1 \quad x_2 \quad \cdots \quad x_n]$,

Операція подвоєння

Для реалізації операції подвоєння потрібно провести операцію суми точки з собою ж.

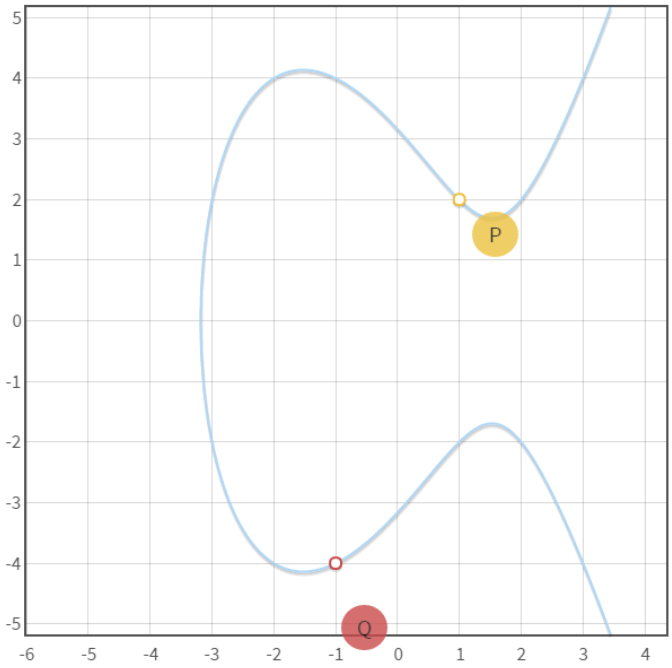


Рисунок 4.7 – Результат подвоєння точки

$$y^2 = x^3 - 7x + 10,$$
$$P(1, 2),$$
$$Q(-1, -4)$$

Тепер запишемо геометричне рішення системою рівняннь:

$$\begin{cases} x = S^2 - 2x_1, \\ y = -y_1 + S(x_1 - x), \\ S = \dfrac{3x_1^2 + a}{2y_1} \end{cases}$$

Визначимо цю систему для загального випадку еліптичної кривої, визначеної у n вимірах:

$$\begin{cases} X = S^2 - 2X_1, \\ y = -y_1 + S(X_1 - X), \\ S = \dfrac{3X_1^2 + A}{2y_1} \end{cases}$$

Множення точки на число

Так само як в звичайній математиці, операція множення є багаторазовим повторенням операції суми. У даному випадку, множенням точки на число є точка, для якої було реалізовано n-разове подвоєння:

$$\boldsymbol{G = nP = \sum_{1}^{n} P}$$

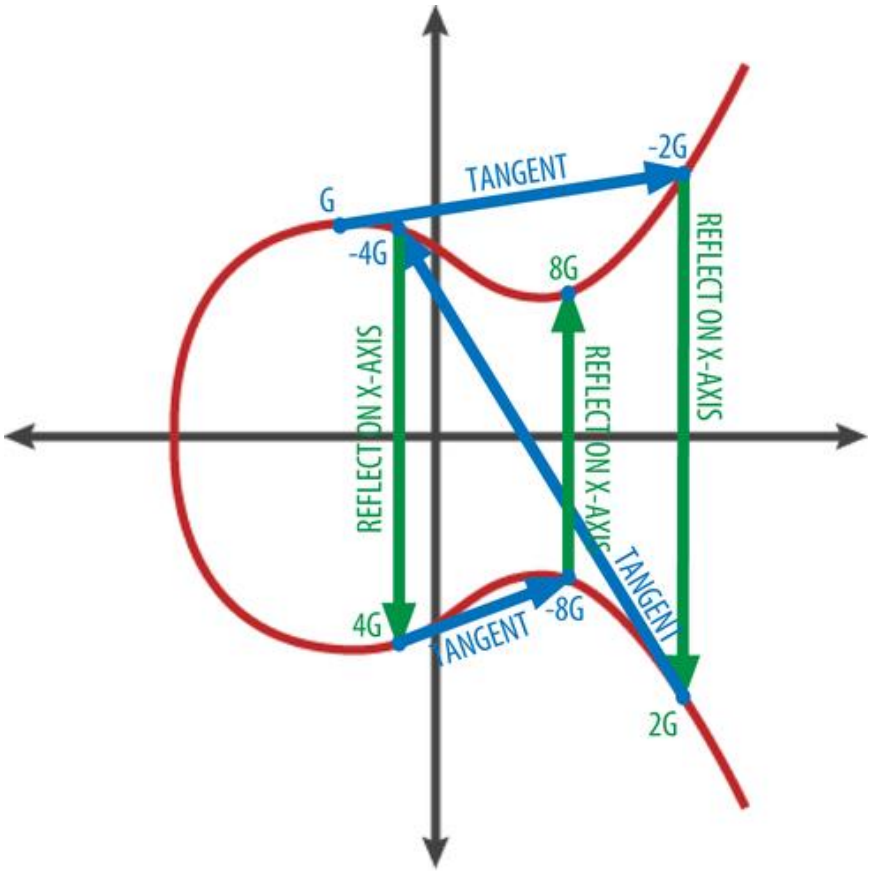


Рисунок 4.8 – Демонстрація алгоритму добутку точки на число

Приклад:

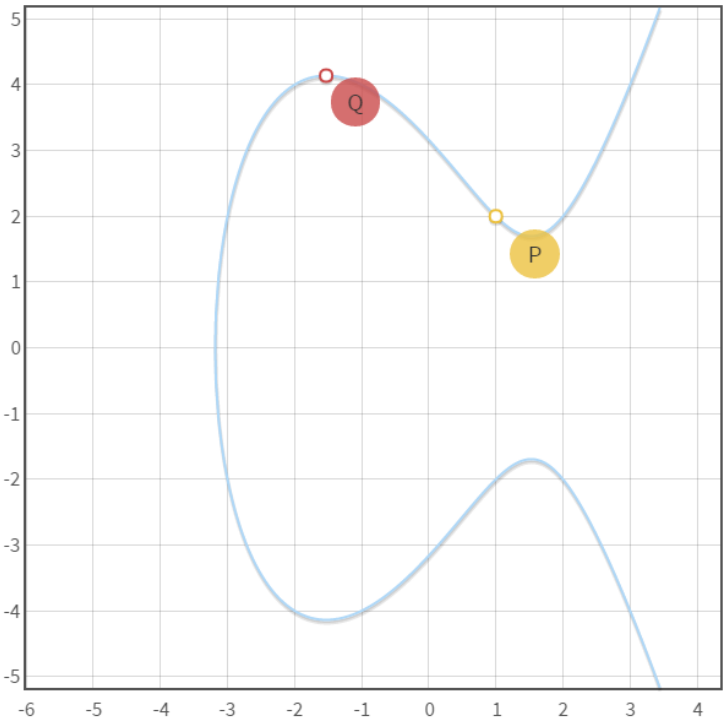


Рисунок 4.9 – Добуток точки і числа

$$\mathbf{y^2 = x^3 - 7x + 10},$$

$$\mathbf{P(1, 2), n = 8},$$

$$\mathbf{Q(-1.52891, 4.13865)}$$

Крива над скінченним полем

Кривою над скінченним полем називається множина цілих точок кривої по модулю простого числа p. Це просте число називається порядком поля. Для кривої над скінченним полем виконуються такі ж операції, що я для звичайної еліптичної кривої, тільки з однією відмінністю: кожна операція виконується по модулю порядка поля.

Збільшення кількості вимірів, у яких визначена еліптична крива призводить до суттєвого збільшення кількості точок у групі, яку створює крива в скінченному полі. Криптостійкість алгоритмів електронного цифрового підпису прямо пропорційно залежить від кількості точок у групі еліптичної кривої над скінченним полем Галуа.

Нижче наведений графік кількості точок в групах отриманих з кривих визначений у двох і трьох вимірах зі збільшенням порядку скінченного поля.

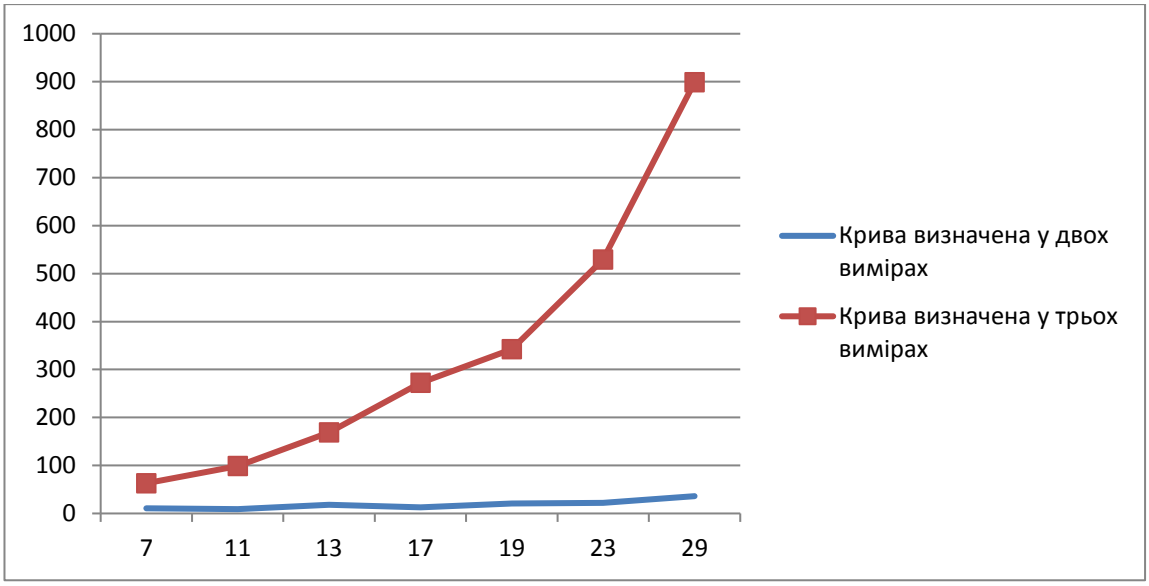


Рисунок 4.10 – Графік кількості точок зі збільшенням порядку кривої

Приклади:

Оберемо криву:

$$\mathbf{y^2 = x^3 + 2x + 3}$$

Порядком кривої оберемо просте число

$$\mathbf{p = 97}$$

У даної кривої над скінченним полем порядку $\mathbf{p = 97}$ існує 100 цілих точок, як видно з рисунку, включаючи нескінченно віддалену.

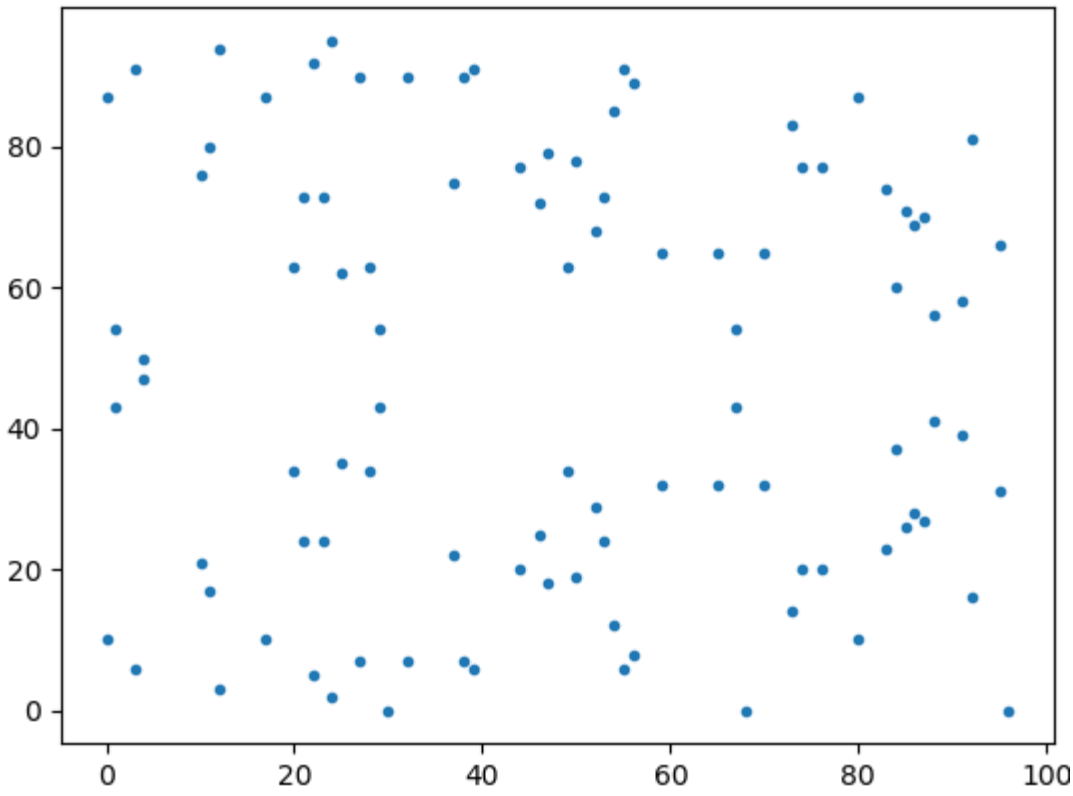


Рисунок 4.11 – Точки кривої, визначеної у двох вимірах

Тепер візьмемо криву, визначену у 3 вимірах:

$$z^2 = x^3 + y^3 + 2x - 2y + 3$$

Взявши той самий параматр порядку скінченного поля отримаємо 9507 точок, що продемонстровано на рисунку.

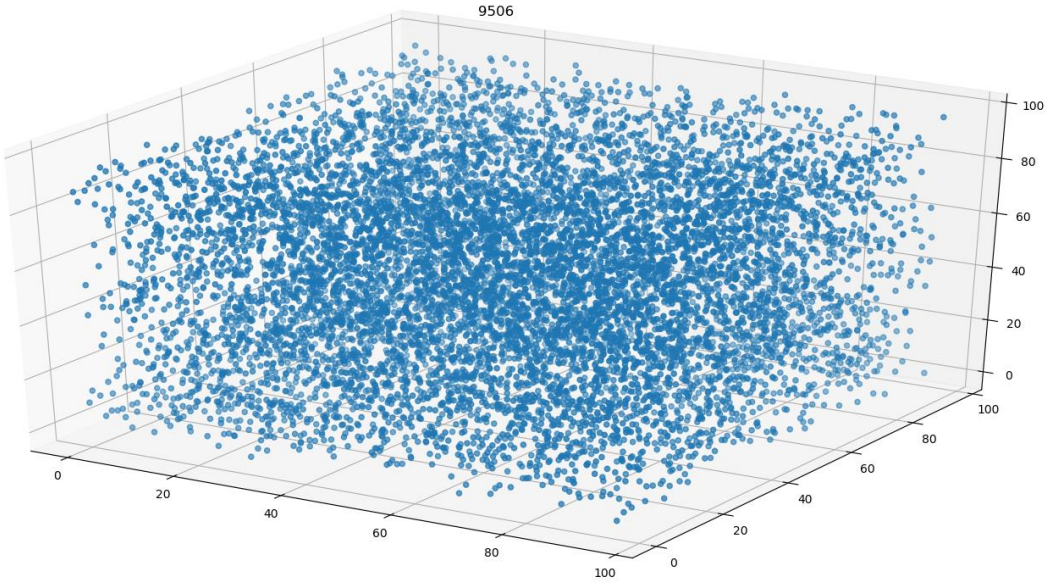


Рисунок 4.12 – Точки кривої, визначеної у трьох вимірах

Операції з точками еліптичної кривої у скінченному полі Галуа визначені також тільки для точок кривої, визначеної у двох вимірах. Було розроблено операції з точками еліптичної кривої визначеної у n вимірах, над скінченним полем. На рисунку 4.13 можна побачити операцію суми точок кривої визначеної у двох вимірах над скінченним полем.

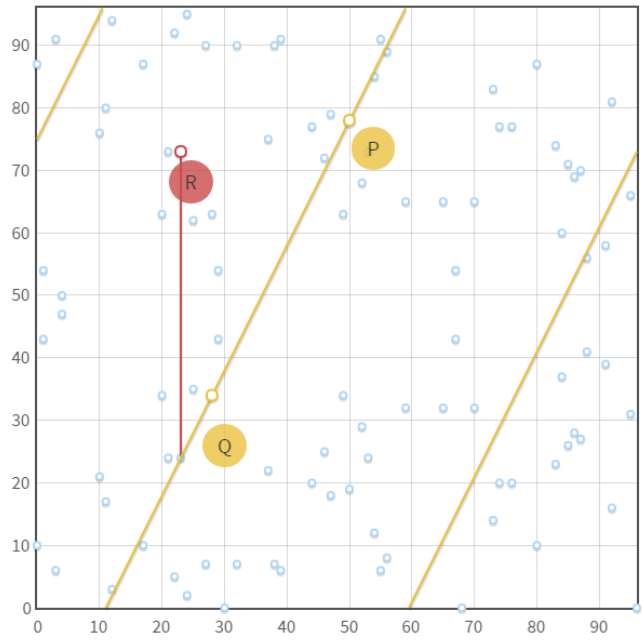


Рисунок 4.13 – Сума точок кривої над скінченним полем

Сума точок загального вигляду еліптичної кривої визначеної у n вимірах над скінченним полем матиме наступний вигляд:

$$\begin{cases} X = S^2 - X_1 - X_2 \ (mod\ p), \\ y = -y_1 + S(X_1 - X) \ (mod\ p), \\ S = \dfrac{y_1 - y_2}{X_1 - X_2} \ (mod\ p) \end{cases}$$

При множенні двох протилежних по осі абсцис точок отримуємо нескінчено віддалену:

$$\mathrm{P} = (74{,}20), \mathrm{P}^{-1}(74{,}77),$$
$$\mathrm{P} + \mathrm{P}^{-1} = \mathrm{O},$$
$$\mathrm{O} = (\infty, \infty)$$

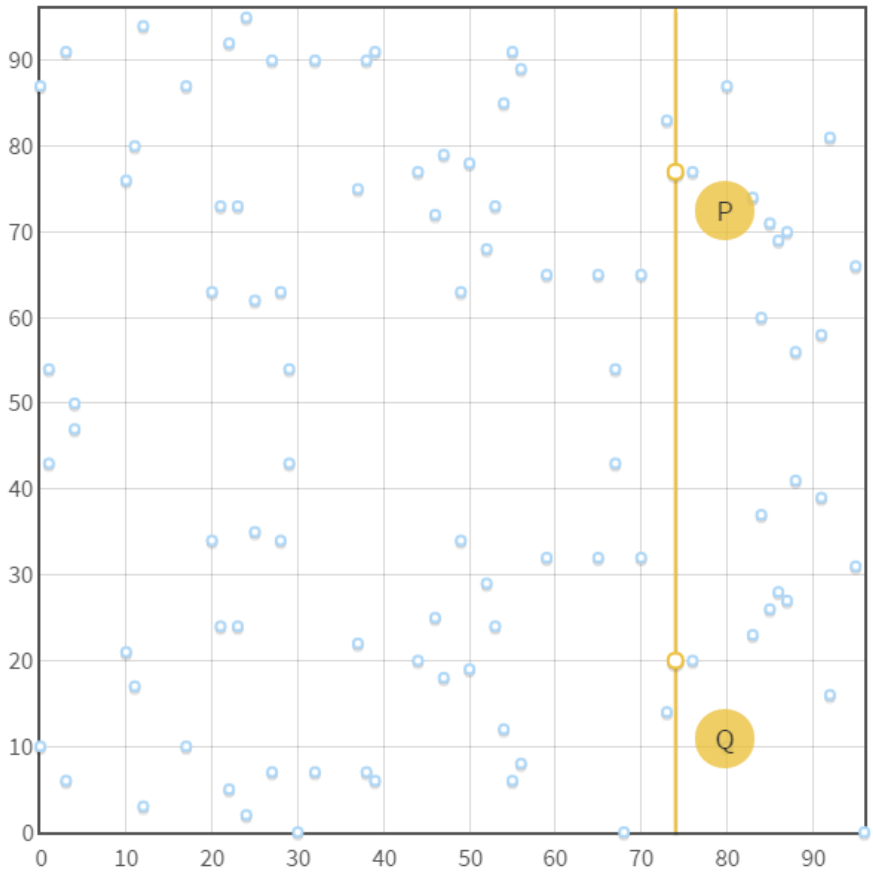


Рисунок 4.14 – Сума двох протилежних точок

Змінивши порядок кривої до $p = 997$ можна отримати 982 точки. А змінивши кількість вимірів у яких визначена крива до трьох і визначивши порядок $p = 97$ отримаємо 9507 точок, що означає, що вже на цьому рівні вибір більшої кількості вимірів покращує результат у сотню разів.

Тепер просумуємо точки кривої, визначеної у двох вимірах та з порядком скінченного поля рівним 997:

$$\mathrm{P} = (172{,}293), \mathrm{Q} = (482{,}578)$$

Отримана точка R в результаті суми має координати:

$$\mathrm{R} = \mathrm{P} + \mathrm{Q}, \mathrm{R} = (632{,}860)$$

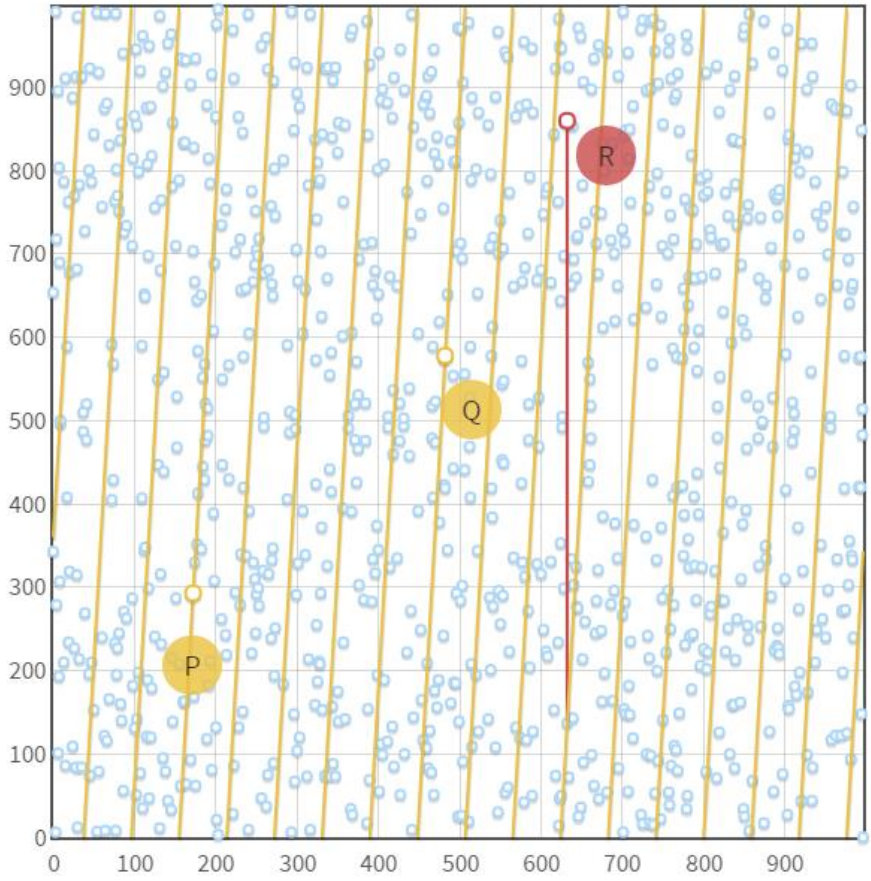


Рисунок 4.15 – Операція суми на полі порядку 997

Операція подвоєння

Операція подвоєння відрізняється від операції подвоєння над множиною дійсних чисел тільки тим, що у множині точок скінченного поля усі операції проводяться по модулю порядку поля.

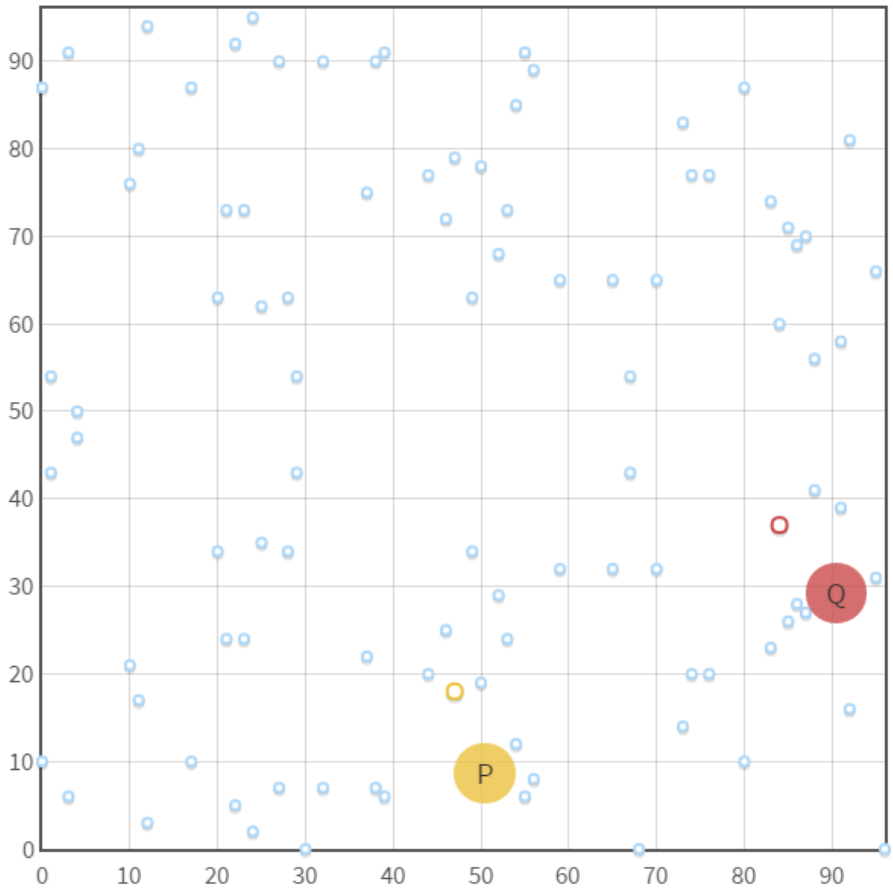


Рисунок 4.16 – Операція подвоєння точки кривої над скінченним полем

Множення точки на число над скінченним полем

У множенні точки на число між точками еліптичної кривої визначеної у двох вимірах над множиною дійсних чисел і точками еліптичної кривої над скінченним полем є різниця у тому, що точки кривої над скінченним полем при множенні на число утворюють кільце певного розміру. Поділивши кількість точок поля на розмір кільця завжди в результаті вийде ціле число, яке називається кофактором точки. Чим кофактор менше, тим більше кільце утворює операція множення точки на число. Для прикладу візьмемо криву, визначену у двох вимірах:

$$y^2 = x^3 + 2x + 3$$

Та поле порядку $p = 97$

В якому визначено 100 цілих точок над скінченним полем, включаючи нескінченно віддалену точку, точка:

$$P(47,18)$$

Створює підгрупу з 50 точок.

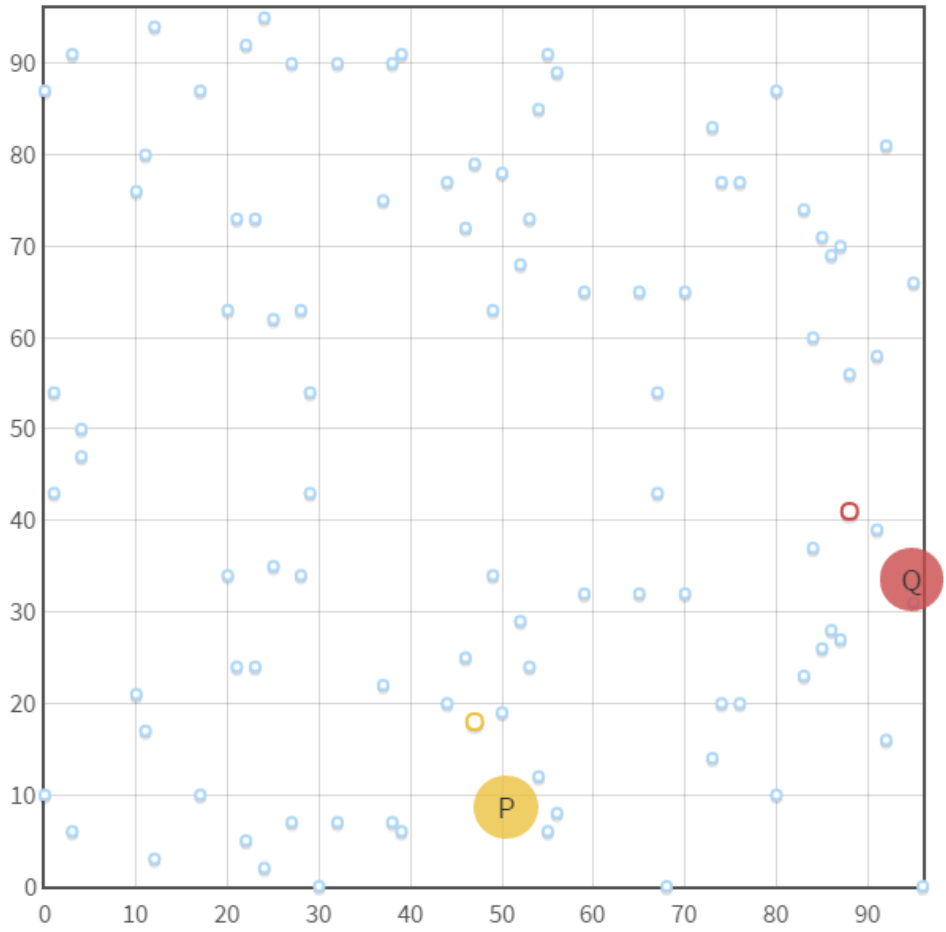


Рисунок4.17 – Множення точки на 5

На Рис. 4.17 наведено приклад множення точки $P(47,18)$ на число 5

А помноживши на 51, знов отримаємо початкове число:

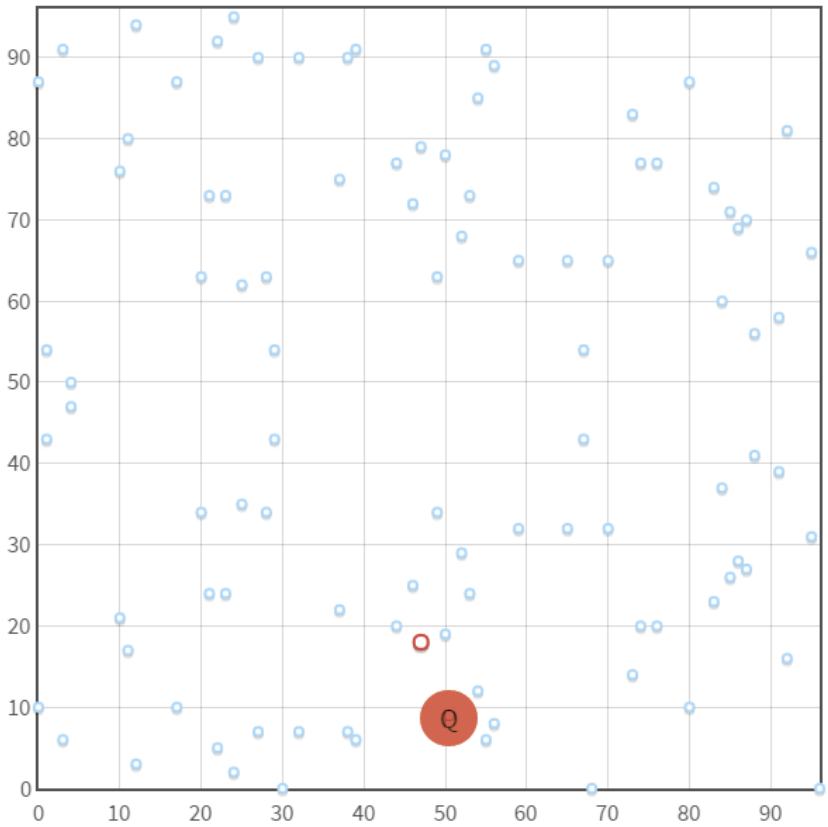


Рисунок 4.18 – Множення точки на 51

А точка:

$$P(74,20)$$

Створює підгрупу з 25 точок. Якщо помножимо P на 25 то отримаємо нескінчено віддалену точку, а з множенням на 26 – знову точку P. На рисунку наведено приклад множення точки P на 8:

$$nP = Q,$$
$$n = 8; P(74,20); Q(52,29).$$

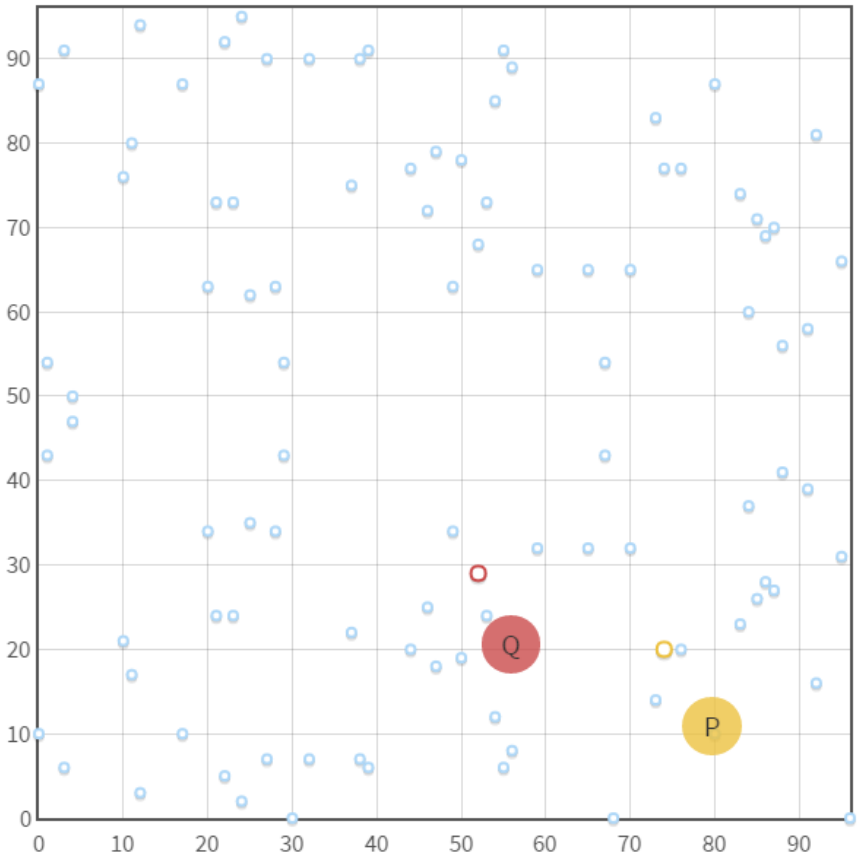


Рисунок 4.19 – Множення точки P на 8

Для того, щоб зберегти рівень криптостійкості для базової точки кривої, від якої проводитимуться операції електронного цифрового підпису повинні реалізовуватися такі вимоги. Для базової точки кофактор повинен бути не більшим за 4. Найкращим варіантом є той, коли кофактор рівний одиниці. У такому випадку в алгоритмі цифрового підпису алфавітом будуть усі точки, які визначені у скінченному полі.

Візьмемо знову криву:

$$y^2 = x^3 + 2x + 3$$

На цей раз порядок поля візьмемо рівним $p = 131$.

Крива над скінченним полем порядку p створює групу цілих чисел кількістю 140, включаючи нескінчено віддалену точку. Точка

$$P(30,48)$$

є базовою. Тобто підгрупа, яку створює операція множення починаючи від точки P має 140 елементів, і охоплює усі точки кривої, що визначені над скінченним полем.

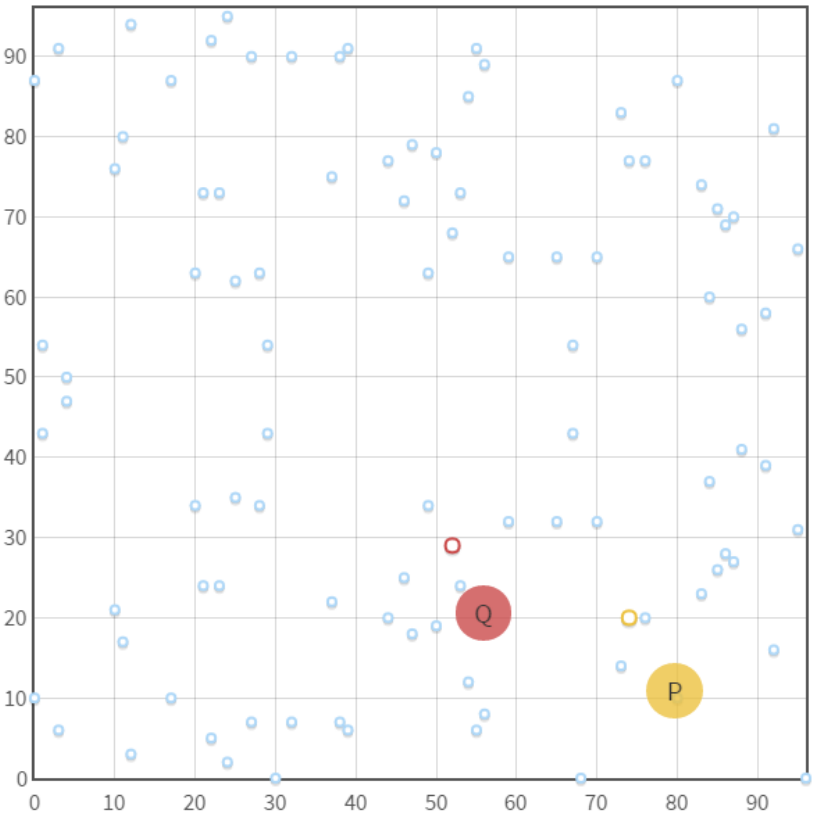


Рисунок 4.20 – Множення базової точки на число

На рисунку операція множення базової точки на число $n = 35$.

5. РОЗРОБКА СЦЕНАРІЇВ ВИКОРИСТАННЯ СИСТЕМИ

Система аутентифікації має трьох типів користувачів і реалізована на додатку А.

Перший тип це користувачі, які завантажили систему для зберігання, генерування паролів та реалізації аутентифікації на базі еліптичних кривих.

Другий тип користувачів це власники веб-сайтів які реалізують процес аутентифікації використовуючи API системи аутентифікації.

Третій тип це користувачі веб ресурсів, в яких реалізація аутентифікації створена за допомогою даної системи аутентифікації.

Діаграму сценаріїв наведено у додатку.

Детальний опис кожного прецеденту діаграми.

Таблиця 5.1

Назва	Створити пароль
ID	1
Опис	Користувач має можливість створити новий пароль у системі зберігання паролю
Актори	Користувач програми
Частота використання	Низька
Тригери	Натискання кнопки створити пароль
Прекондиції	Завантажена версія програми, запущена програма
Посткондиції	Створений новий пароль
Головний курс	1. Натиснути на кнопку створити пароль 2. Записати пароль 3. Записати повторний ввід паролю 4. Натиснути на кнопку зберегти
Альтернативний курс	1. Натиснути на кнопку створити пароль 2. Записати пароль

	3. Записати повторний ввід паролю 4. Натиснути на кнопку відмінити
Помилки	Повторний ввід паролю не співпадає з першим – пароль не збережеться

Таблиця 5.2

Назва	Згенерувати пароль
ID	2
Опис	Користувач має можливість згенерувати новий пароль у системі зберігання паролю
Актори	Користувач програми
Частота використання	Низька
Тригери	Натискання кнопки згенерувати пароль
Прекондиції	Завантажена версія програми, запущена програма
Посткондиції	Створений новий пароль
Головний курс	1. Натиснути на кнопку згенерувати пароль 2. Натиснути на кнопку зберегти
Альтернативний курс	1. Натиснути на кнопку згенерувати пароль 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити пароль не збережеться

Таблиця 5.3

Назва	Створити пару ключів
ID	3
Опис	Користувач має можливість згенерувати пару ключів системі реалізації аутентифікації
Актори	Користувач програми
Частота використання	Низька

Тригери	Натискання кнопки згенерувати пару ключів
Прекондиції	Завантажена версія програми, запущена програма
Посткондиції	Створена нова пара ключів
Головний курс	1. Натиснути на кнопку згенерувати пару ключів 2. Натиснути на кнопку зберегти
Альтернативний курс	1. Натиснути на кнопку згенерувати пару ключів 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити пара ключів не збережеться

Таблиця 5.4

Назва	Зберегти пароль до менеджеру
ID	4
Опис	Користувач має можливість зберегти ключі до менеджеру паролів
Актори	Користувач програми
Частота використання	Середня
Тригери	Натискання кнопки зберегти
Прекондиції	1/2/3
Посткондиції	Збережені дані
Головний курс	1. Натиснути на кнопку зберегти в одному з вікні створення паролів 2. Натиснути кнопку зберегти
Альтернативний курс	1. Натиснути на кнопку зберегти в одному з вікні створення паролів 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити пароль не

	збережеться

Таблиця 5.5

Назва	Записати пароль до буферу обміну
ID	5
Опис	Користувач має можливість записати обраний пароль до буферу обміну
Актори	Користувач програми
Частота використання	Висока
Тригери	Натискання гарячої клавіші
Прекондиції	4
Посткондиції	Обраний пароль запишеться до буферу обміну
Головний курс	1. Натиснути на гарячу клавішу знаходячись у будь-якому вікні 2. Обрати з списку що відкрився потрібний пароль
Альтернативний курс	1. Натиснути на гарячу клавішу знаходячись у будь-якому вікні 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити пароль не запишеться

Таблиця 5.6

Назва	Записати публічний ключ до буферу обміну
ID	6
Опис	Користувач має можливість записати обраний публічний ключ до буферу обміну
Актори	Користувач програми
Частота використання	Висока

Тригери	Натискання гарячої клавіші
Прекондиції	3
Посткондиції	Обраний публічний ключ запишеться до буферу обміну
Головний курс	1. Натиснути на гарячу клавішу знаходячись у будь-якому вікні 2. Обрати з списку що відкрився потрібний публічний ключ
Альтернативний курс	1. Натиснути на гарячу клавішу знаходячись у будь-якому вікні 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити публічний ключ не запишеться

Таблиця 5.7

Назва	Провести операцію ЕЦП
ID	7
Опис	Користувач має можливість реалізувати операцію електронного цифрового підпису з обраною парою ключів
Актори	Користувач програми
Частота використання	Висока
Тригери	Натискання кнопки ЕЦП
Прекондиції	3
Посткондиції	Користувач отримає цифровий підпис даних
Головний курс	1. Натиснути на кнопку ЕЦП 2. Обрати з списку що відкрився потрібну пару ключів 3. Вставити текст або обрати потрібний файл

Альтернативний курс	1. Натиснути на кнопку ЕЦП 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити операція ЕЦП не реалізується

Таблиця 5.8

Назва	Згенерувати скрипт аутентифікації
ID	8
Опис	Користувач має можливість згенерувати скрипт аутентифікації для свого веб-ресурсу
Актори	Власник Веб-сайту
Частота використання	Низька
Тригери	Натискання кнопки згенерувати скрипт
Прекондиції	Обраний тариф користування системою
Посткондиції	Користувач отримає скрипт для реалізації аутентифікації на власному сайті
Головний курс	1. Натиснути на кнопку згенерувати скрипт 2. Заповнити необхідні поля 3. Вставити скрипт в код сторінки сайту
Альтернативний курс	1. Натиснути на кнопку згенерувати скрипт 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити скрипт не реалізується

Таблиця 5.9

Назва	Створити пару ключів
ID	9
Опис	Користувач має можливість згенерувати пару ключів

Актори	Користувач
Частота використання	Середня
Тригери	Натискання кнопки згенерувати пару ключів
Прекондиції	Відкритий сайт системи
Посткондиції	Користувач отримає пару ключів, серед яких публічний ключ запишеться до списку публічних ключів
Головний курс	1. Натиснути на кнопку згенерувати пару ключів 2. Заповнити необхідні поля 3. Завантажити ключі
Альтернативний курс	1. Натиснути на кнопку згенерувати пару ключів 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити ключі не згенеруються

Таблиця 5.10

Назва	Завантажити приватний ключ
ID	10
Опис	Користувач має можливість завантажити приватний ключ з веб-саайту
Актори	Користувач Веб-сайту
Частота використання	Висока
Тригери	Натискання кнопки реєстрація
Прекондиції	Відкритий сайт
Посткондиції	Користувач отримає пару ключів, серед яких публічний ключ запишеться до списку публічних ключів

Головний курс	1. Натиснути на кнопку реєстрація 2. Заповнити необхідні поля 3. Завантажити ключ
Альтернативний курс	1. Натиснути на кнопку реєстрація 2. Натиснути на кнопку відмінити
Помилки	Натиснувши на кнопку відмінити ключі не згенеруються

Таблиця 5.11

Назва	Здійснити аутентифікацію
ID	11
Опис	Користувач має можливість здійснити аутентифікацію
Актори	Користувач Веб-сайту
Частота використання	Висока
Тригери	Відкриття сайту
Прекондиції	10
Посткондиції	Користувач після відкриття сайту одразу стає зареєстрованим
Головний курс	1. Відкрити сайт
Помилки	Відсутній файл з ключем на пристрої не дасть змогу залогінитись

6. РОЗРОБКА СТРУКТУРНОЇ СХЕМИ СИСТЕМИ

Структурну схему можна побачити в додатку Б

Структурна схема складається з наступних модулів:

- модуль серверної частини ,
- модуль інтерфейсу користувача,
- модуль генерування паролю,
- модуль електронного цифрового підпису,
- модуль аутентифікації.

Модулі між собою з'єднані мережевою моделлю TCP/IP.

В модулі серверної частини аутентифікації реалізована база даних.

Для кращого розуміння структурної схеми розроблено дві функціональні схеми:

- функціональна схема підсистеми менеджеру паролів реалізована в додатку В,
- функціональна схема підсистеми двофакторної аутентифікації реалізована в додатку Г.

Функціональна схема підсистеми менеджеру паролів містить чотири модулі:

- модуль серверної частини,
- модуль інтерфейсу користувача,
- модуль генерування паролю,
- модуль електронного цифрового підпису.

Модуль інтерфейсу користувача складається з:

- налаштування властивостей паролю,
- налаштування облікового запису,
- менеджеру паролів,
- системи підпису/провірки ЕЦП,
- створення пари ключів.

Користувач має доступ тільки до модулю інтерфейсу корисутвача. Взаємодія з модулем генерування паролів реалізується через налаштування властивостей паролю.

Модуль генерування паролю складається з:

- генератора псевдовипадкових чисел,
- генератора паролю.

Взаємодія з модулем електронного цифрового підпису реалізується з модулю інтерфейсу користувача через систему підпису /провірки ЕЦП та створення пари ключів.

Модуль електронного цифрового підпису містить:

- алгоритм перевірки коректності цифрового підпису,
- алгоритм реалізації цифрового підпису,
- генератору пари ключів.

Згенерований публічний ключ після створення зберігається модулем серверної частини через менеджер публічних ключів до бази даних.

Функціональна схема підсистеми двофакторної аутентифікації містить наступні модулі:

- модуль аутентифікації,
- модуль серверної частини системи аутентифікації.

Користувач має доступ до модулю аутентифікації, у якого є наступні функції:

- налаштування облікового запису,
- система підпису/провірки ЕЦП,
- створення пари ключів,
- шифрування/дешифрування інформації.

З функцій налаштування облікового запису, системи підпису/провірки ЕЦП, створення пари ключів інформація може потрапити до модулю серверної частини після шифрування.

Модуль серверної частини містить наступні функції:

- шифрування/дешифрування інформації,
- алгоритм перевірки коректності цифрового підпису,
- генератор пари ключів,
- алгоритм реалізації цифрового підпису,
- менеджер роботи з базою даних.

Через функцію менеджера публічних ключів реалізується запис до бази даних.

Отримана інформація після дешифрування може обробитися однією з функцій:

- генератором пари ключів, після чого до модулю аутентифікації повернеться згенерована пара ключів, якою користувач після дешифрування зможе користуватися. Генератором пари ключів, через менеджер роботи з базою даних створюється запис з новою парою ключів користувача.
- Алгоритмом реалізації цифрового підпису, після отримання запиту на підпис, проводиться алгоритм електронного цифрового підпису, після чого результат зашифровується і відправляється до модулю аутентифікації.
- Алгоритмом перевірки коректності цифрового підпису, отримавши запит на підтвердження коректності електронного цифрового підпису, функція через менеджер роботи з базою даних отримує публічний ключ користувача і проводиться перевірка. Отриманий результат зашифровується і відправляється до модулю аутентифікації.

7. РОЗРОБКА ER ДІАГРАМИ БАЗИ ДАНИХ

Діаграма сутність-зв’язок знаходиться у додатку Д.

Діаграма містить наступні сутності:

- користувач,
- токен,
- ключ,
- веб-сайт.

Від сутності користувач унаслідувані наступні сутності:

- преміум користувач,
- користувач Веб-сайту,
- власник веб-сайту.

Зв’язок один до багатьох між наступними парами сутностей:

- користувач – ключ,
- користувач – токен,
- власник веб-сайту – веб-сайт,
- веб-сайт – користувач веб-сайту.

Сутність користувач має наступні атрибути:

- ID – первинний ключ,
- ім’я,
- пароль,
- дата реєстрації,
- номер телефону.

Сутність преміум користувач має наступні атрибути:

- дата закінчення.

Сутність токен має наступні атрибути:

- ID – первинний ключ,
- токен.

Сутність ключ має наступні атрибути:

- ID – первинний ключ,
- публічний ключ.

Сутність веб-сайт має наступні атрибути:

- ID – первинний ключ,
- адреса.

8. СТАРТАП-ПРОЕКТ

8.1. Опис ідеї проекту

Ідея стартапу полягає в створенні програмного продукту для реалізації операції аутентифікації на базі еліптичних кривих визначених у трьох вимірах, генерування та зберігання паролів. Унікальність продукта полягає у вищій криптостійкості електронного цифрового підпису зі збереженням швидкодії.

Таблиця 8.1. Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
	1. Менеджер паролів	Безпечне зберігання паролів Можливість генерування складних паролів Швидкий вибір потрібного паролю
	2. Система аутентифікації на електронний ресурс	Можливість реалізації двофакторної аутентифікації на базі системи Генерування пари ключів для реалізації ЕЦП на базі еліптичної кривої для другого фактору аутентифікації
	3. Система аутентифікації для особистого користування	Генерування пари ключів для реалізації ЕЦП на базі еліптичної кривої для особистого

		користування Список публічних ключів усіх користувачів системи, для можливості перевірки коректності підпису

Таблиця 8.2. Визначення си чльних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	(Потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	LastPass	JaCarta WebPass	ZShell			
1.	Створення пари ключів	Присутнє	Відсутнє	Присутнє	Присутнє	-	+	-
2.	Використання кривих визначених у 3 вимірах	Присутнє	Відсутнє	Відсутнє	Відсутнє	-	-	+
3.	Можливість застосування смарт-карт	Відсутня	Відсутня	Присутня	Відсутня	+	-	-
4.	Можливість використання через мережу інтернет	Присутня	Присутня	Відсутня	Присутня	-	+	-
5.	Можливість застосування на різних ОС	Присутня	Присутня	Присутня	Відсутня	-	+	-

№ п/п	Техніко-економічні характеристики ідеї	(Потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	LastPass	JaCarta WebPass	ZShell			
6.	Генератор паролів	Присутній	Відсутній	Відсутній	Відсутній	-	-	+
7.	Менеджер паролів	Присутній	Присутній	Відсутній	Присутній	-	-	+
8	Двофакторна аутентифікація	Присутня	Присутня	Присутня	Присутня	-	+	-

8.2. Технологічний аудит ідеї проекту

Таблиця 8.3. Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
4.		Компільована у машинний код (C++)	Наявні	Доступні
5.		Компільована у байткод (C#)	Наявні	Доступні
6.		Скриптова/інтерпретована (Python)	Наявні	Доступні
Обрана технологія реалізації ідеї проекту: Скриптова/інтерпретована (Python)				

8.3. Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 8.4. Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	5
2	Загальний обсяг продаж, грн/ум.од	500 грн/ум. од.
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Недискримінаційні якісні
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6	Середня норма рентабельності в галузі (або по ринку), %	73%

Таблиця 8.5. Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
Управління паролями	1. Особисте користування 2. Малий бізнес	Управління особистими, корпоративними паролями	Збільшення безпеки унеможливлення розкриття даних через людський фактор
Реалізація двофакторної аутентифікації	1. Малий бізнес 2. Середній бізнес	Наявність вимог до криптостійкості	Гнучкість у налаштуванні аутентифікації індивідуально для кожного клієнта

Таблиця 8.6. Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Крадіжка інтелектуальної власності	Крадіжка ідеї або ключової інтелектуальної інновації	Відсудження прав інтелектуальної власності Попередження користувачів із подальшою співпрацею для мінімізації фактор загрози
2.	Отримання несанкціонованого доступу сторонніми	Хакерська атака що може призвести до компроментації даних клієнтів	Залучення спеціалістів з інформаційної безпеки Попередження користувачів із подальшою співпрацею для

	особами		мінімізації фактор загрози
3.	Відсутність ринку	Відсутність шляху збуту товару внаслідок помилкового орієнтування	Ретельний розгляд проблем потенційних клієнтів Залучення експертів та менторів Консультації із спеціалістами
4.	Недостача капіталовкладень	Витрачені усі кошти до моменту виходу на ринок	Пошук нових джерел інвестицій

Таблиця 8.7. Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1.	Отримання інвестицій	Отримання капіталу що необхідний для реалізації продукту	Розробка продукту
2.	Успішна маркетингова політика	В результаті проведеної маркетингової політики отримана висока зацікавленість користувачів	Підтримка стабільної роботи системи та проведення масштабування системи Збільшення цін на використання сервісу Використання подібної маркетингової стратегії надалі для залучення нових користувачів
3.	Поглинання конкурентами	Пропозиція купівлі проекту або розроблених технологій одним із	Розвиток розроблених технологій Оцінка вартості розроблених технологій

		конкурентів	

Таблиця 8.8. Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
Олігополія	Незначна кількість конкурентів Велика ринкова сила Схожість використовуваних технологій	Інформування ринку щодо появи нової платформи управління хмарною інфраструктурою
Галузевий	Загроза появи нових конкурентів Висока потреба у товарі	Інформування ринку щодо якості використовуваної новаторської технології Пропозиція гнучких цін
Внутрішньогалузева	Діяльність в одній галузі економіки Надання сервісів одного типу	Зменшення вартості сервісу Примноження каналів розподілу
Товарно-видова	Надання різних сервісів одного типу	Маркетингова політика
Цінова	Використання цін для покращення економічних умов збуту	Зменшення вартості платформи Використання нових каналів розподілу

Марочна	Пропозиція схожої платформи Спільна цільова аудиторія	Інформування ринку щодо появи нової платформи управління хмарною інфраструктурою

Таблиця 8.9. Аналіз конкуренції в галузі за М. Портером

Складові аналізу		Висновки
Прямі конкуренти в галузі	LastPass, JaCarta WebPass, ZShell	CR4 = 92% Індекс Херфіндаля-Хіршмана (HHI) = 6565 Значення показників вказує на високу концентрацію (монополізацію) даного ринку
Потенційні конкуренти	Розмір капіталовкладень, Забезпечення гнучких цін, Доступ до каналів розподілу, Витрати на масштабах	Можливості входу на ринок забезпечить мінімізація цін, швидкість та простота надавання послуги споживачам і співпраця із головними гравцями ринку. В результаті аналізу проектів на народно-громадських інтернет-платформах потенційних конкурентів знайдено не було

Постачальники	Відсутні	Відсутні
Клієнти	Змінні витрати: Виробничі непрямі дегресивні - Системи інформації: пропаганда, реклама та директ-маркетинг, - Рівень чутливості до цін: споживачі орієнтовані на цінність продукту - Продуктова диференціація: якість, спосіб отримання сервісу, швидкість обслуговування Методи контролю якості: тестування та профілювання, прототипування, інспектування коду, аналіз архітектури програмного забезпечення	Клієнти диктують умови гнучкості цінової політики, високої і довгострокової якості послуг та наявність кооперації із сервісами, що вони використовують
Товари-замінники	Копіювання функціоналу, Монополізація дистриб'юторів, Демпінгування	Пропонування вигідних умов дистриб'юторам, забезпечення захисту інтелектуальної власності, гнучкість цінової політики

Таблиця 8.10. Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1.	Унікальність сервісу	Розроблений продукт має унікальні пропозиції: генератор паролів, Реалізація ЕЦП на базі еліптичних кривих визначених у 3 вимірах
2.	Цінова політика	Отримання прибутку здійснюється за рахунок гнучкої моделі оплати
3.	Модель “бізнес для бізнесу”	Бізнес модель грунтується на унікальності пропозиції і співпраці з власниками веб ресурсів. Даний підхід дозволить обійти цінову конкуренцію на ринку цільової аудиторії

Таблиця 8.11. SWOT- аналіз стартап-проекту

Сильні сторони: Унікальність пропозиції Низькі ціни	Слабкі сторони: Нестача капіталовкладень Відсутність можливості використання смарт-карт
Можливості: Інвестиції Висока зацікавленість цільової аудиторії	Загрози: Крадіжка інтелектуальної власності Компроментація даних клієнтів Відсутність ринку

Таблиця 8.12. Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Розшерення можливостей сервісу	Ймовірне	6 місяців
2.	Додання нових бізнес моделей	Малоймовірне	8 місяців
3.	Пошук бізнесів інших галузей для співпраці	Малоймовірне	6 місяців
Обрана альтернатива: Розшерення можливостей сервісу			

8.4. Розроблення ринкової стратегії проекту

Таблиця 8.13. Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Користувачі персональних комп'ютерів	Висока	65%	Середня	Низькі бар’єри входу
2.	ІТ-підрозділи середнього бізнесу	Мала	42%	Середня	Високі бар’єри входу
3.	Власники	Висока	76%	Середня	Низькі

	веб-сайтів				бар’єри входу
Які цільові групи обрано: Користувачі персональних комп'ютерів, Власники веб-сайтів					

Таблиця 8.14. Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	Надання платформи малому та середньому бізнесу	Вибірковий розподіл	Здатність протистояти прямим конкурентам Низькі витрати Ефективна співпраця	Стратегія диференціації

Таблиця 8.15. Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1	Ні	Забирати та залучати нових	Веб-інтерфейс системи керування	Стратегія лідера. Розширення первинного попиту

Таблиця 8.16. Визначення стратегії позиціонування

Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
Відповідність затвердженим характеристикам Висока ступінь надійності системи Простий інтерфейс	Стратегія диференціації	Формування регулярного попиту Збільшення разового використання послуги Виявлення нових	Інноваційність технології Низькі ціни Простота використання

адміністратора Гнучка цінова політика Оперативна підтримка продукту		груп споживачів Нові напрями застосування існуючої послуги	

8.5. Розроблення маркетингової програми стартап-проекту

Таблиця 8.17. Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Створення криптостійких паролів	Генератор паролів	Якість надання послуг Простота використання
2	Двофакторна аутентифікація	Реалізація двофакторної аутентифікації на базі ЕЦП	Якість надання послуг Інноваційність технологій що використовуються Простота використання
3	Безпечність зберігання паролів	Простий і зручний менеджер паролів	Якість надання послуг Простота використання

Таблиця 8.18. Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
І. Товар за задумом	Програмний продукт що надає можливість облегшити аутентифікацію і збільшити криптостійкість		
	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	Кількість		1 шт.
	Якість: стандарти якості постачання програмних продуктів		
	Пакування: Завантеження з інтернет ресурсу		
	Марка: MultiPass		
	Програмний продукт		
	Програмний продукт, технічна підтримка та підписка на оновлення		
За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності			

Таблиця 8.19. Визначення меж встановлення ціни

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
3 – 4 usd./міс.	3 – 10 usd./міс.	20 000 грн./міс.	2 – 3 usd./міс.

Таблиця 8.20. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Закупівля здійснюється через довірені джерела	Інформування користувачів Доступ	Канал одного рівня	Селективна з використанням комбінованого

	користування сервісом		каналу збуту

Таблиця 7.21. Концепція маркетингових комунікацій

Специфіка поведінки цільових клієнтів	Автоматизація бізнес-процесів Вимоги до високодоступності та відмовостійкості
Канали комунікацій, якими користуються цільові клієнти	Прямі офіційні
Ключові позиції, обрані для позиціонування	Послідовність в реалізації обраної позиції Доступність та об’єктивність інформації про фірму і товар Унікальність послуги
Завдання рекламного повідомлення	Формування у цільової аудиторії обізнаності про появу нового продукту Інформування користувачів про властивості та переваги продукту Інформування користувачів про нові способи використання відомого продукту Пояснення цільовій аудиторії принципу роботи платформи Виправити у користувачів неправильні представлення про продукт
Концепція рекламного звернення	Раціоналістична стратегія реклами

ВИСНОВКИ

Метою дисертації було створення системи аутентифікації з підвищеним рівнем криптостійкості за рахунок збільшення кількості вимірів у яких визначена еліптична крива, та збереження швидкості роботи за рахунок використання векторних операцій.

Система аутентифікації містить робочу програму користувача, в якій є можливість генерування та запису необмеженої кількості паролів, їх безпечне зберігання та швидкий доступ. Також робоча програма користувача містить модуль генерування пари публічного та приватного ключів для особистого користування.

Іншим модулем системи є серверна частина, яка містить алгоритми електронного цифрового підпису на базі еліптичних кривих, визначених у трьох вимірах. Серверна частина також містить скрипт для використання власниками сайтів для впровадження двофакторної аутентифікації за допомогою електронного цифрового підпису.

Виконуючи задачі дисертації було досліджено переваги алгоритмів реалізації електронного цифрового підпису на базі еліптичних кривих визначених у більшій кількості вимірів. Провівши дослідження було зроблено висновок, що еліптична крива визначена у трьох вимірах має значно більшу кількість точок у скінченному полі ніж крива, визначена у двох вимірах. Більша кількість точок у скінченному полі прямо пропорційна більшій криптостійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Koblitz N. Introduction to Elliptic Curves and Modular Forms / Koblitz., 1993. – (2).

2. Schneier, Bruce. Applied Cryptography, John Wiley & Sons, 1994

3. Miller V.C. Use og Elliptic Curve in Cryptography // Cryptology: Proceedings of Crypto 85, Springer LNCS 218, 1986. – P. 417-426.

4. Daniel R. L. Brown. Generic Groups, Collision Resistance, and ECDSA / Daniel R. L. Brown., 2002.

5. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

6. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Nakamoto., 2008.

7. Antonopoulos A. Mastering Bitcoin - Unlocking Digital Cryptocurrencies / Antonopoulos., 2014.

8. Винберг Э. Б. Курс алгебры. — новое изд., перераб. и доп. — М. : МЦНМО, 2011. — 592 с. — 2000 прим.

9. What is an ECC (Elliptic Curve Cryptography) certificate? [Електронний ресурс]. – 11. – Режим доступу до ресурсу: https://www.namecheap.com/support/knowledgebase/article.aspx/9503/38/what-is-an-ecc-elliptic-curve-cryptography-certificate.

10. R De Groote. The number of points on an elliptic cubic curve over a finite field / R De Groote, J Hirschfeld., 1980. – (1).

11. Schoof R. Nonsingular plane cubic curves over finite fields / René Schoof // Nonsingular plane cubic curves over finite fields / René Schoof., 1987. – (A). – С. 183–211.

12. Layman's Guide to Elliptic Curve Digital Signatures [Електронний ресурс] // The Royal Fork. – 2014. – Режим доступу до ресурсу: http://royalforkblog.github.io/2014/09/04/ecc/.

13. Цифровая подпись. Эллиптические кривые [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: https://www.osp.ru/os/2002/07-08/181696/.

14. ДСТУ 4145-2002. Інформаційні технології ; Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння / О. Шаталов (розроб.)Кочубінський А. (розроб.). - Офіц. вид. - К. : Державний комітет України з питань технічного регулювання та споживчої політики, 2003. - V, 31 с. - (Національний стандарт України). - Бібліогр.: с. 30.

15. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації / І.Д. Горбенко, Т.О. Гріненко; Харк. нац. ун-т радіоелектрон. - Х., 2004. - 368 с. - Бібліогр.: 73 назв. - укр.

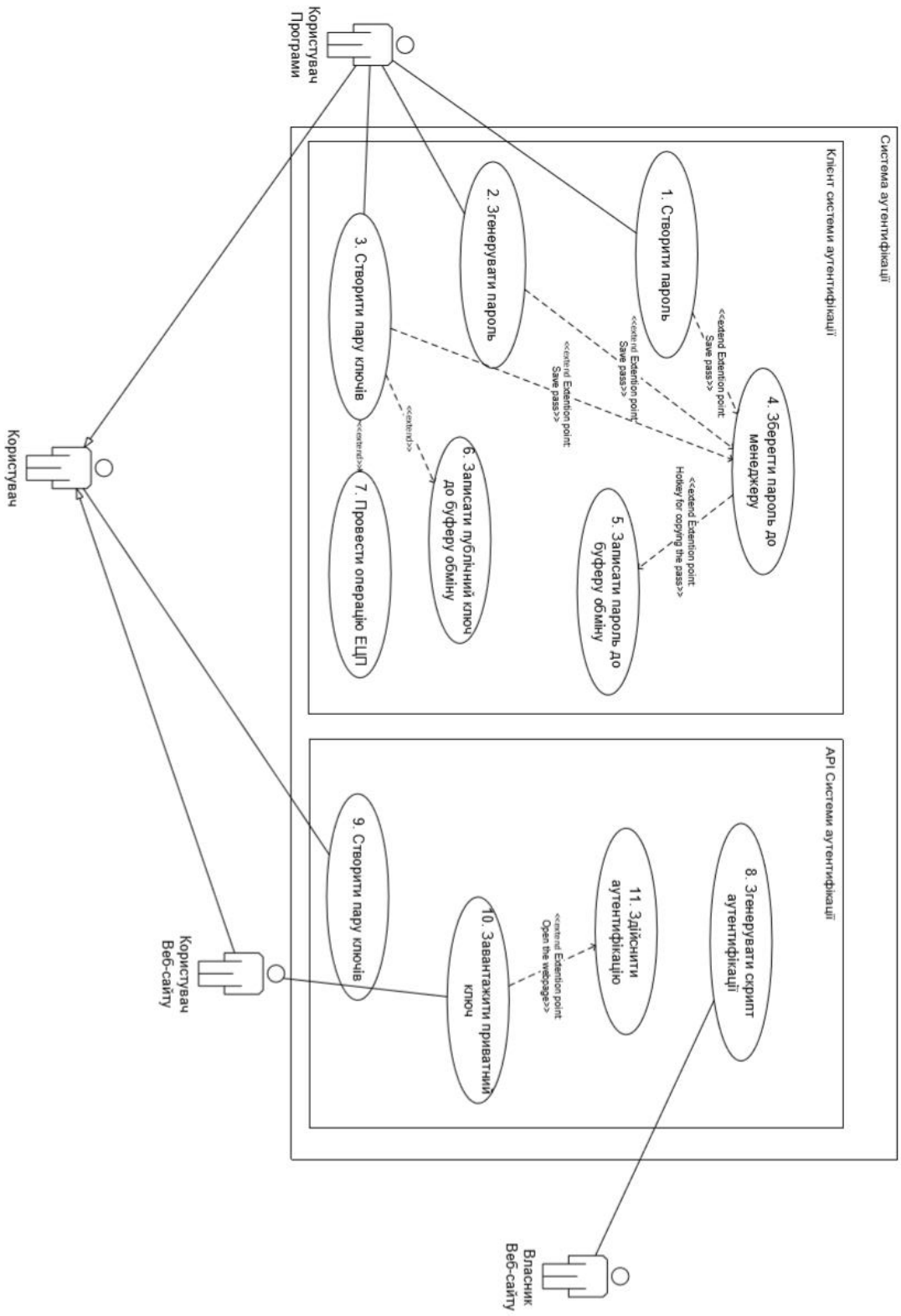
16. Моделі і системи оцінювання, обробки та захисту фінансової інформації : Моногр. / Г.М. Азаренкова, С.В. Гадецька, І.Д. Горбенко, Ю.В. Дубницький, О.О. Єгоршин; Ред.: О.В. Васюренко. - Х.: Константа, 2005. - 380 с. - Бібліогр.: с. 368-380. - укр.

17. Система аутентифікації [Електронний ресурс]. https://www.aladdin-rd.ru/catalog/jacarta-u2f

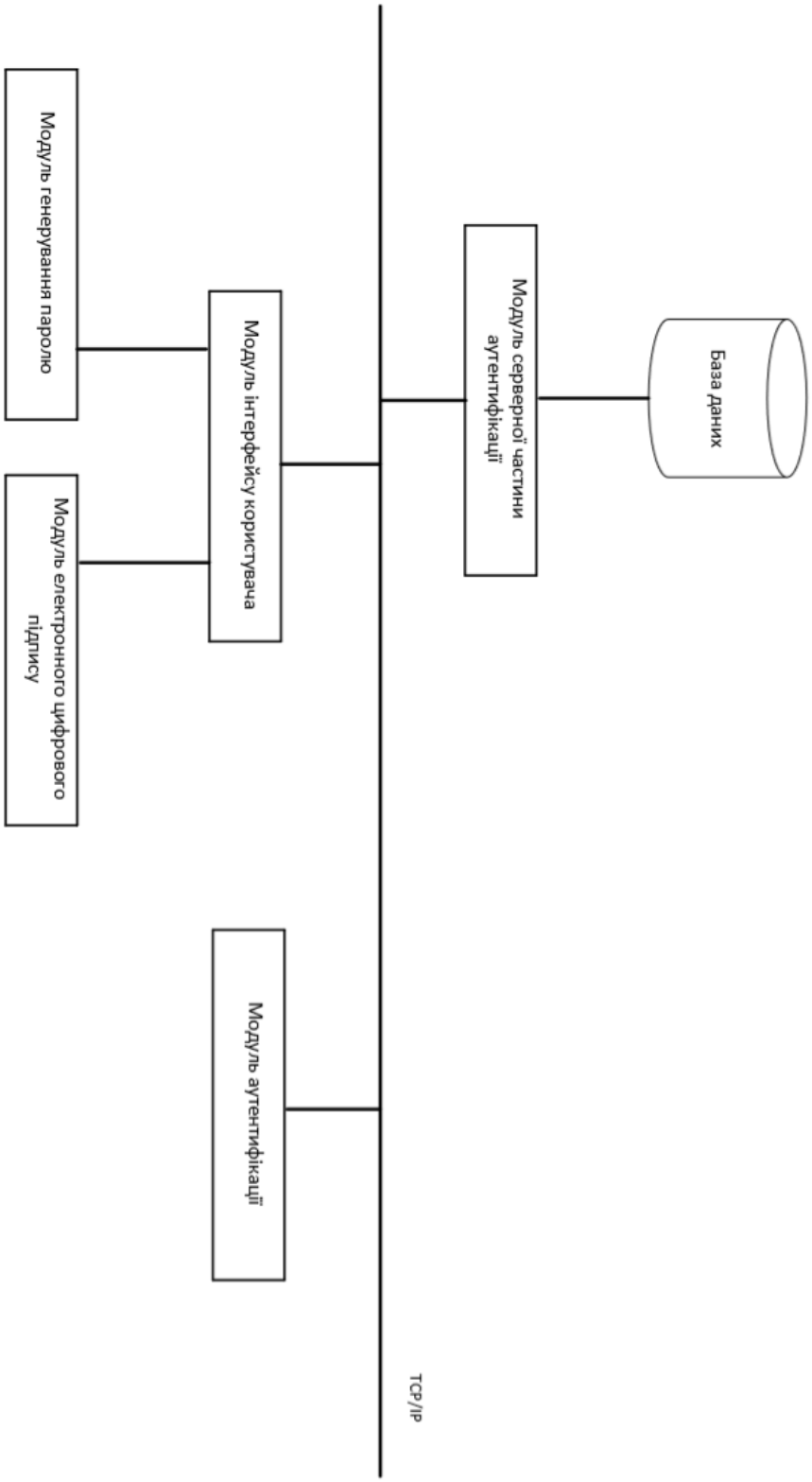
18. Accredited Standards Committee X9 Incorporated Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) Paperback – 2005

19. Thomas R. ShemanskeModern Cryptography and Elliptic Curves: A Beginner's Guide (Student Mathematical Library) / Thomas R. Shemanske – 2017 – 252c.

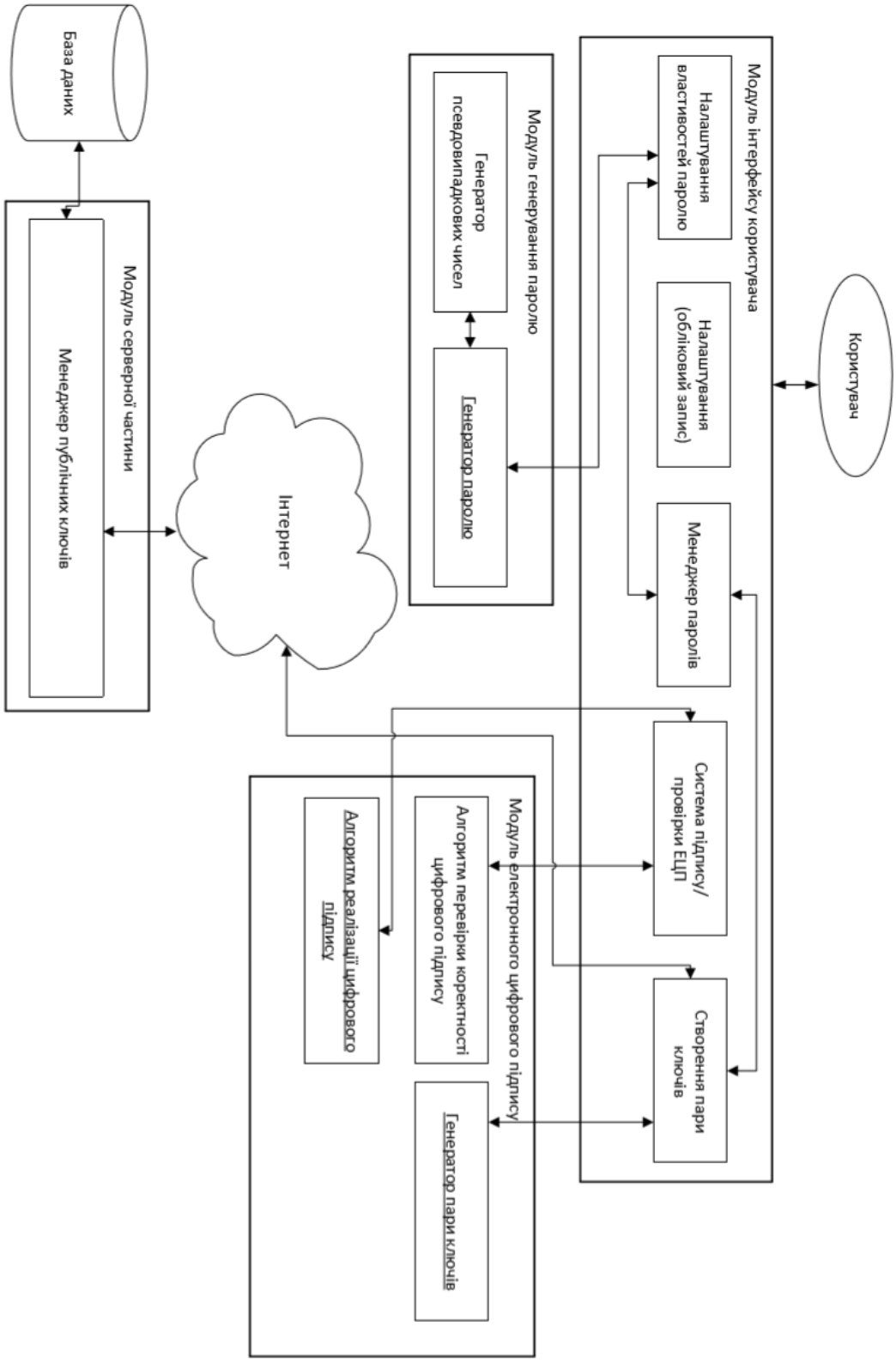
ДОДАТОК А


Користувач Програми
Користувач
Користувач Веб-сайту
Власник Веб-сайту
Система аутентифікації
Клієнт системи аутентифікації
1. Створити пароль
2. Згенерувати пароль
3. Створити пару ключів
4. Зберегти пароль до менеджеру
5. Записати пароль до буферу обміну
6. Записати публічний ключ до буферу обміну
7. Провести операцію ЕЦП
<<extend Extention point: Save pass>>
<<extend Extention point: Save pass>>
<<extend Extention point: Save pass>>
<<extend Extention point: Hotkey for copying the pass>>
<<extend>>
<<extend>>
API Системи аутентифікації
8. Згенерувати скрипт аутентифікації
9. Створити пару ключів
10. Завантажити приватний ключ
11. Здійснити аутентифікацію
<<extend Extention point: Open the webpage>>

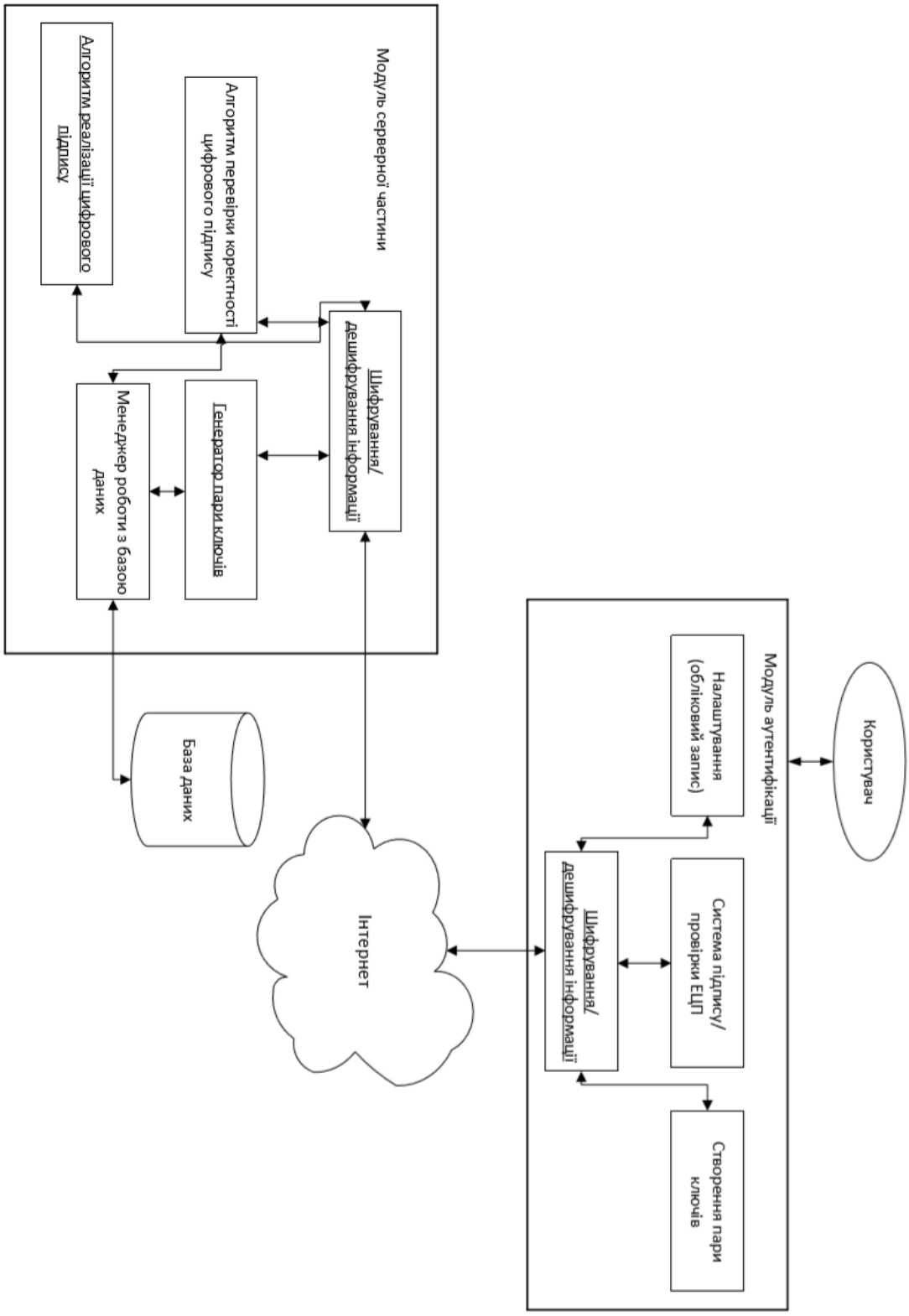
ДОДАТОК Б


TCP/IP
Модуль аутентифікації
Модуль інтерфейсу користувача
Модуль генерування паролю
Модуль електронного цифрового підпису
Модуль серверної частини аутентифікації
База даних

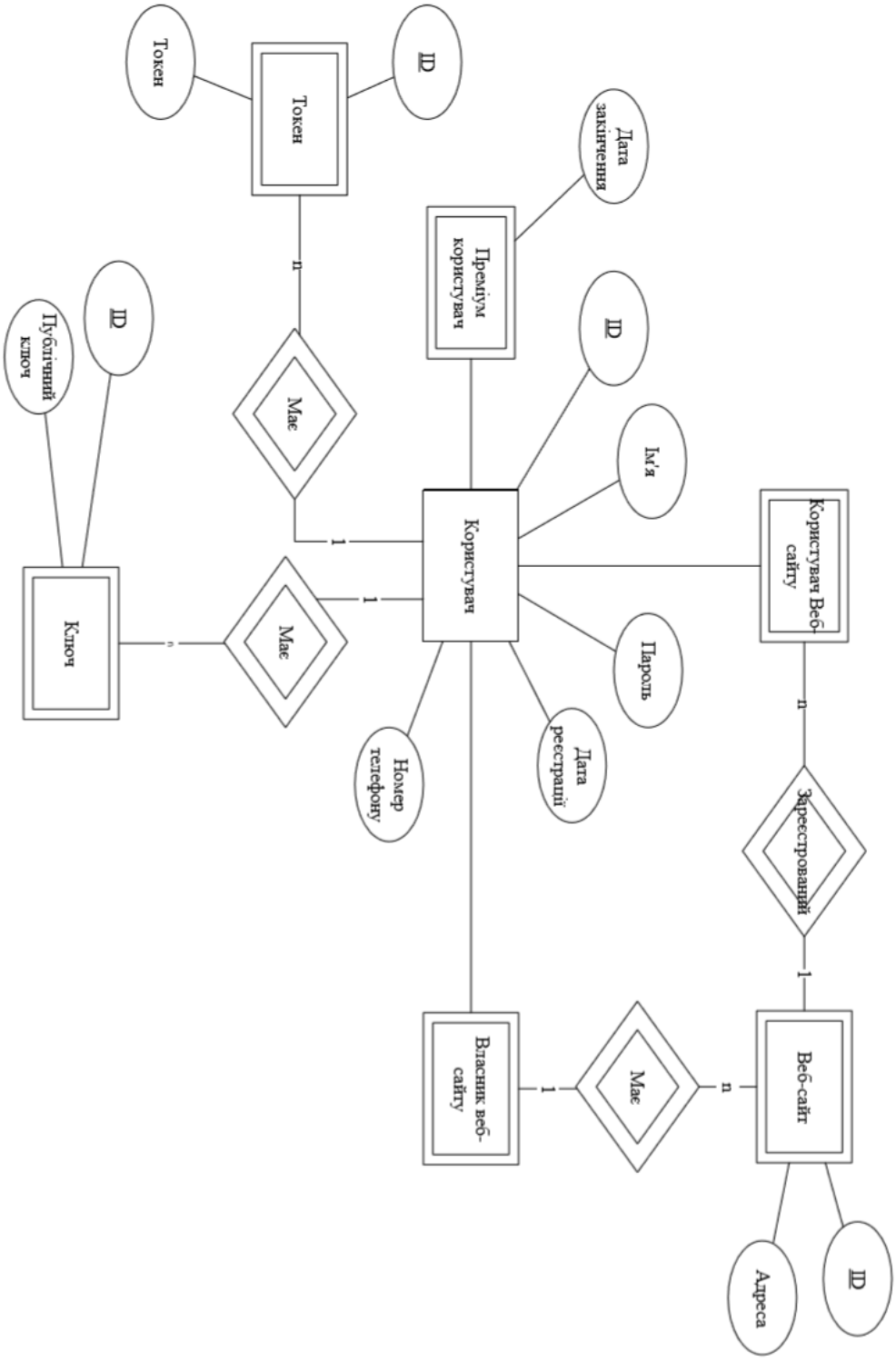
ДОДАТОК В


Користувач
Модуль інтерфейсу користувача
Налаштування властивостей паролю
Налаштування (обліковий запис)
Менеджер паролів
Система підпису/ провірки ЕЦП
Створення пари ключів
Модуль генерування паролю
Генератор псевдовипадкових чисел
Генератор паролю
Модуль електронного цифрового підпису
Алгоритм реалізації цифрового підпису
Алгоритм перевірки коректності цифрового підпису
Генератор пари ключів
Інтернет
Модуль серверної частини
Менеджер публічних ключів
База даних

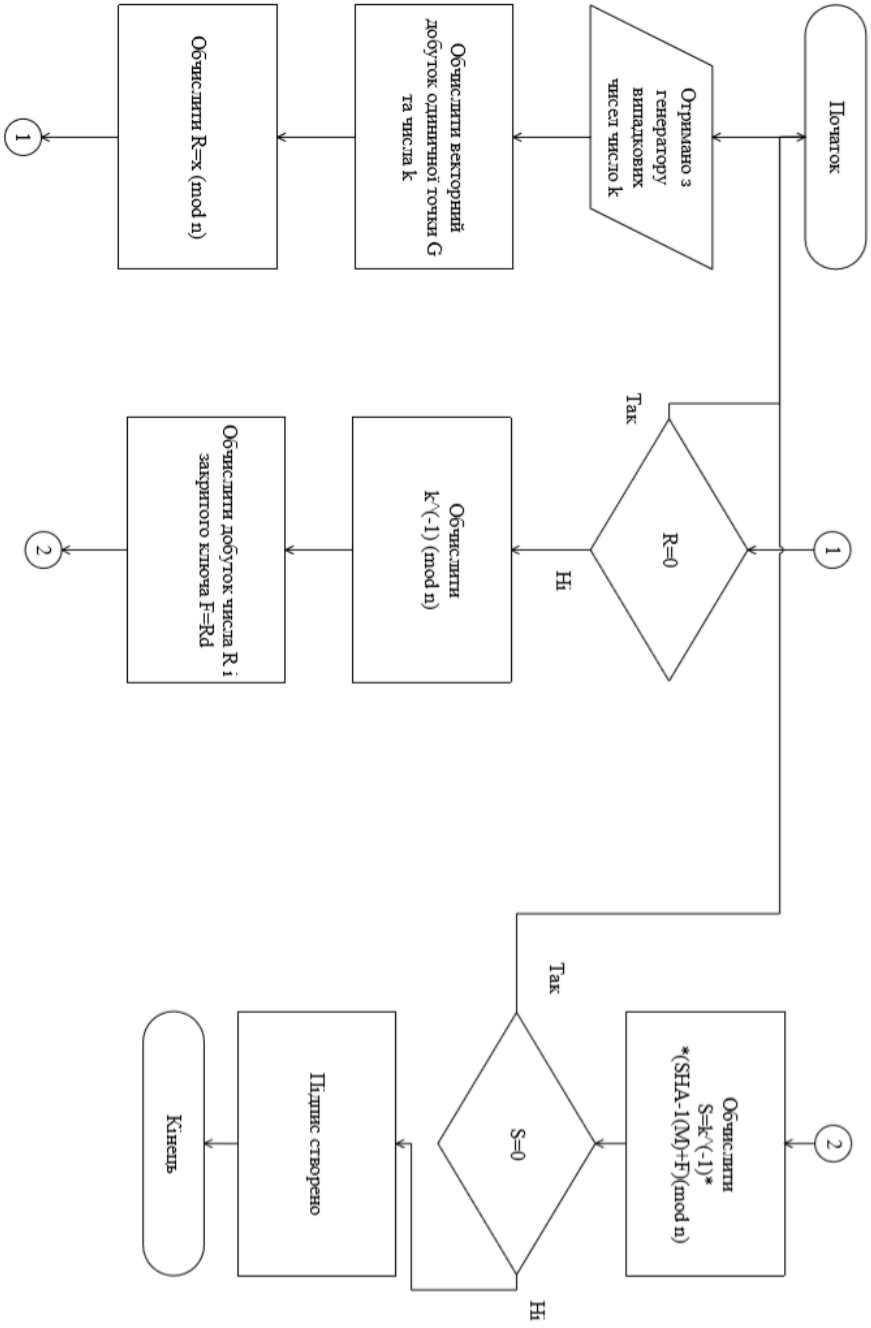
ДОДАТОК Г


Користувач
Модуль аутентифікації
Налаштування (обліковий запис)
Система підпису/ провірки ЕЦП
Створення пари ключів
Шифрування/ дешифрування інформації
Інтернет
Модуль серверної частини
Шифрування/ дешифрування інформації
Генератор пари ключів
Менеджер роботи з базою даних
Алгоритм перевірки коректності цифрового підпису
Алгоритм реалізації цифрового підпису
База даних

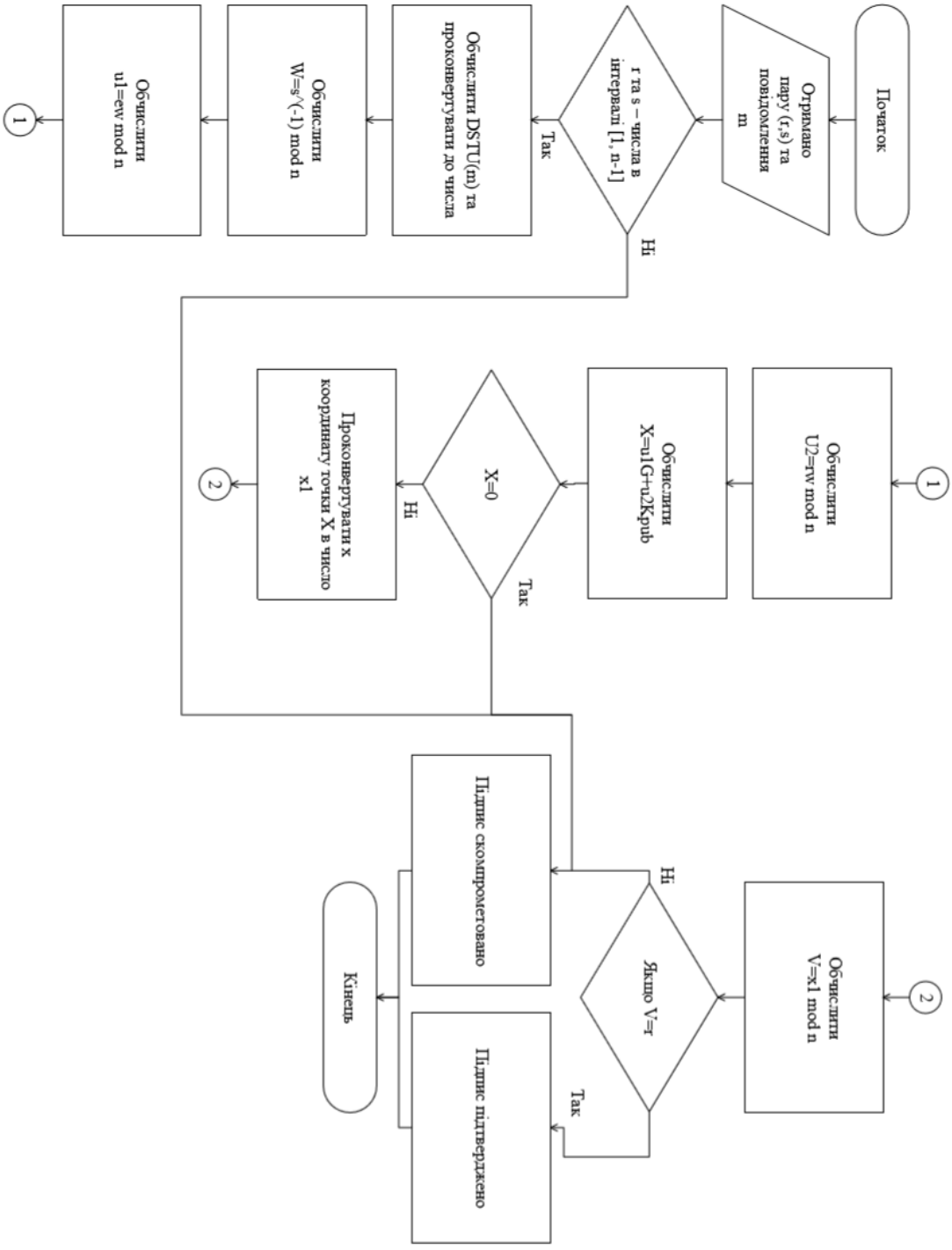
ДОДАТОК Д


Токен
ID
Токен
Дата закінчення
Премиум користувач
ID
Ім'я
Користувач Веб-сайту
Пароль
Дата реєстрації
Номер телефону
Користувач
Публічний ключ
ID
Ключ
Має
Має
Має
Зареєстрований
Власник веб-сайту
Веб-сайт
Адреса
ID
1
n
1
1
n
1
n
1
n

ДОДАТОК Ж


Початок
Отримано з генератору випадкових чисел число k
Обчислити векторний добуток одиничної точки G та числа k
Обчислити R=x (mod n)
1
R=0
Так
Ні
Обчислити k^(-1) (mod n)
Обчислити добуток числа R і закритого ключа F=Rd
2
2
Обчислити S=k^(-1)*(SHA-1(M)+F)(mod n)
S=0
Так
Ні
Підпис створено
Кінець

ДОДАТОК К


Початок
Отримано пару (r,s) та повідомлення m
r та s – числа в інтервалі [1, n-1]
Так
Ні
Обчислити DSTU(m) та проконвертувати до числа
Обчислити W=s^(-1) mod n
Обчислити u1=ew mod n
1
Обчислити U2=rw mod n
Обчислити X=u1G+u2Kpub
X=0
Так
Ні
Проконвертувати x координату точки X в число x1
2
Обчислити V=x1 mod n
Якщо V=r
Так
Ні
Підпис підтверджено
Підпис скомпрометовано
Кінець

ДОДАТОК Л

Початок
Генерування приватного ключа Бобом та Алісою Kpriv=rand(1, n)
Генерування публічного ключа Бобом та Алісою Kpub=Kpriv*Q
Обмін публічними ключами та множення отриманого публічного ключа на свій приватний, отримана точка одна: Z=Kpriv1*Kpriv2*Q
Отримана точка проходить через односторонню функцію
Аліса вводить повідомлення для шифрування m
1
Проводиться шифрування C=m*Z mod n
Зашифроване повідомлення відправляється по незахищеному каналу
Боб, отримавши повідомлення дешифрує його m=c Z^(-1) mod n
2
2
Якщо повідомлення несе інформацію
Ні
Так
Проводиться запит на повторне відправлення
Розшифрування готове
Кінець